PART 2

1

Engagement Planning

Module

1	Engagement Objectives, Scope, and Evaluation Criteria	3
2	Topical Requirements and Strategic Objectives	15
3	IT Considerations	25
4	Business Continuity and Disaster Recovery	49
5	Finance and Accounting Concepts	59
6	Key Risks and Controls Related to Business Processes	71
7	Appropriate Engagement Approach	101
8	Performing a Detailed Risk Assessment	117
9	Engagement Procedures	133
10	Engagement Resources and Skills	147

© Becker Professional Education Corporation. All rights reserved.

MODULE

1 Engagement Objectives, Scope, and Evaluation Criteria

Part 2
Unit 1

This module covers the following topics from the *CIA examination syllabus*:

CIA Syllabus—Section A: Engagement Planning

1. Determine engagement objectives and scope

   May include but is not limited to:

   a. Recognize how to apply Topical Requirements when determining objectives and scope

   b. Recognize elements to be considered in the development of engagement objectives, including regulatory requirements; the organization's strategy and objectives; governance, risk management, and control processes; risk appetite and tolerance; internal policies; previous audit reports; work of other assurance providers; and whether the engagement is intended to provide assurance or advisory services

   c. Identify and document relevant scope limitations during planning

   d. Evaluate approaches for managing and documenting stakeholder requests

   e. Identify effective methods for addressing changes in objectives and scope

2. Determine evaluation criteria based on relevant information gathered

   May include but is not limited to:

   a. Identify the most relevant criteria for evaluating the activity under review

   b. Determine whether a set of evaluation criteria is specific, practical, relevant, aligned with the objectives of the organization and the activity under review, and produces reliable comparisons

© Becker Professional Education Corporation. All rights reserved.

1 Purpose and Objectives

Requirements **Standard 13.3 Engagement Objectives and Scope**

Internal auditors must establish and document the objectives and scope for each engagement.

The engagement objectives must articulate the purpose of the engagement and describe the specific goals to be achieved, including those mandated by laws and/or regulations.

The scope must establish the engagement's focus and boundaries by specifying the activities, locations, processes, systems, components, time period to be covered in the engagement, and other elements to be reviewed and be sufficient to achieve the engagement objectives.

Internal auditors must consider whether the engagement is intended to provide assurance or advisory services because stakeholder expectations and the requirements of the Standards differ depending on the type of engagement.

Scope limitations must be discussed with management when identified, with a goal of achieving resolution. Scope limitations are assurance engagement conditions, such as resource constraints or restrictions on access to personnel, facilities, data, and information, that prevent internal auditors from performing the work as expected in the audit work program.

If a resolution cannot be achieved with management, the chief audit executive must elevate the scope limitation issue to the board according to an established methodology.

Internal auditors must have the flexibility to make changes to the engagement objectives and scope when audit work identifies the need to do so as the engagement progresses.

The chief audit executive must approve the engagement objectives and scope and any changes that occur during the engagement.

Preparing the engagement objectives and scope is part of the engagement planning process. The *Global Internal Audit Standards*™ (the Standards) outline the steps in the engagement planning process as follows:

- Understand the initial expectations and reasons for the engagement.
- Gather information to understand the organization and the activity under review and to assess the risks relevant to the activity.
- Conduct a preliminary engagement assessment of relevant risks, allowing internal auditors to identify and prioritize the risks to determine the engagement objectives and scope.
- Identify the criteria and resources needed to perform the engagement.
- Develop an engagement work program which describes the specific engagement steps to be performed.

© Becker Professional Education Corporation. All rights reserved.

1.1 Assurance vs. Advisory Services

Before establishing the objectives of an engagement, it is helpful to understand the type and purpose of the engagement. The internal audit function may provide assurance or advisory services for different purposes, but the overarching mission of all these activities is to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight. It is helpful for internal auditors to consider the findings of risk assessments prior to establishing objectives.

Assurance services are objective examinations of evidence to provide an objective assessment on governance, risk management, and control processes for the organization. Advisory services are also known as consulting activities, the nature and scope of which are agreed with the client, intended to add value, and improve an organization's governance, risk management, and control processes. These services are provided without the internal audit function acting as management.

1.2 Objectives

After the purpose of an engagement is determined, engagement objectives should be established. Engagement objectives are statements that articulate the purpose of an engagement and describe the specific goals to be achieved.

Internal auditors primarily determine the objectives of assurance engagements. However, advisory engagements are often established jointly by internal auditors and management of the activity or process (i.e., the client) under review.

During engagement planning, internal auditors will perform an engagement risk assessment, which includes identifying and prioritizing risks and helps influence the engagement objectives and scope. The engagement workpapers should include documentation showing the alignment of the objectives and the engagement risk assessment.

With both assurance and advisory engagements, it is critical to understand the expectations of the stakeholders. As noted in the Standards, "The engagement objectives should align the engagement objectives with the business objectives of the activity under review, as well as with those of the organization." Internal auditors confirm the objectives and scope with the management of the activity under review during the engagement opening or entrance meeting and make any changes if needed. Minutes of the meeting with stakeholders about the engagement objectives and scope should be retained as evidence of conformance with the Standards.

Objectives are typically documented in the form of action phrases (e.g., "Determine the operating effectiveness of the three-way match control." or "Evaluate the design adequacy of the whistleblower anonymous reporting program.") and focus on the activities that help mitigate the organization's risks, identified in the engagement risk assessment. The engagement objectives, along with the scope, should be documented in an approved engagement work program.

© Becker Professional Education Corporation. All rights reserved.

Certain elements should be considered when establishing engagement objectives, including:

- **Regulatory Requirements:** When regulatory compliance is required, objectives should include evaluating compliance. Examples include the General Data Protection Regulation (GDPR) in the European Union, the Foreign Corrupt Practices Act (FCPA) in the United States, the UK Bribery Act in the United Kingdom, and Payment Card Industry (PCI) data security standards.
- **The Organization's Strategy and Objectives:** The engagement objectives should reflect the organization's strategy and objectives as a means of enhancing and protecting organizational value.
- **Governance, Risk Management, and Control Processes:** Governance, risk management, and controls are interrelated concepts. Objectives should consider the impacts to each of these individually and in the aggregate.
- **Risk Appetite and Tolerance:** To appropriately evaluate whether risks are sufficiently mitigated, the organization's appetite for risk must be considered when establishing engagement objectives.
- **Internal Policies:** Routine policies and practices often represent control activities. In addition to considering conformance with internal policies, internal auditors may also consider the appropriateness of the policies.
- **Previous Audit Reports:** Previous audit reports reveal process and control deficiencies that were present in the past. Engagement objectives may consider the mitigation of these deficiencies and risks identified in these engagements.
- **Work of Other Assurance Providers:** External auditors may identify deficiencies that internal auditors did not previously identify. Information from these engagements can assist internal auditors in defining engagement objectives.

Illustration 1 Example Engagement Objectives

- Evaluate the design adequacy of the materials price variance review control.
- Determine the operating effectiveness of the bank reconciliation control.
- Assess the data collection and retention policy with respect to GDPR compliance.
- Determine the effectiveness and efficiency of the engineer recruiting and hiring process.
- Evaluate the accuracy of data inputs for the sales commissions and bonus model.
- Assess the achievement of second line risk management goals.
- Determine the performance of recently implemented cost savings strategies in procurement.
- Evaluate the clarity and transparency in the design of compensation and benefits systems for the Argentina acquisition.

© Becker Professional Education Corporation. All rights reserved.

1.2.1 Assurance Engagement Objectives

For assurance engagements that focus on providing assurance of whether controls are designed and operating effectively, the engagement objectives can direct the priorities for testing controls and systems. As provided in the Standards, the objectives can focus on controls designed to manage risks related to:

- Assignment of authority and responsibility.
- Compliance with policies, plans, procedures, laws, and regulations.
- Reporting accurate, reliable information.
- Effectively and efficiently using resources.
- Safeguarding assets.

Pass Key

Engagement objectives are what internal auditors intend to achieve in the engagement and should align with:

- the business objectives of the activity under review and with those of the organization; and
- the engagement risk assessment.

2 Topical Requirements

Topical Requirements are a mandatory element of the International Professional Practices Framework® (IPPF) along with the *Global Internal Audit Standards*. As defined by the IPPF, "Topical Requirements are designed to enhance the consistency and quality of internal audit services related to specific audit subjects and to support internal auditors performing engagements in those risk areas."

Topical Requirements raise the internal audit function's professionalism and performance, improve the quality and value of internal audit services, provide comfort to stakeholders that critical elements are addressed, and complement the *Global Internal Audit Standards* and guidance. They are required and applicable only to specific audit topics or engagements that are designated within an organization's internal audit plan.

Topical Requirements are identified based on the evolving risk landscape across industries and sectors. It is mandatory to incorporate Topical Requirements when an audit engagement covers the identified topic. As described by The Institute of Internal Auditors (The IIA), the Topical Requirements provide a baseline for engagement performance; however, they are not comprehensive work programs.

Each Topical Requirement provides a structure for frequently audited global topics that are typically higher risk and pervasive in nature. They list attributes that must be considered and documented when auditing a relevant subject.

© Becker Professional Education Corporation. All rights reserved.

Internal audit should recognize when the audit area includes these subjects when scoping the engagement because, to the extent that audit areas include one of these subjects, the engagement objectives must reflect the related Topical Requirements.

For an engagement addressing any aspect of the topic, internal auditors must document when they determine that the specific requirements are not applicable, along with the rationale. When there are applicable requirements, internal auditors would include those in the objectives and obtain and document evidence in the workpapers when performing the engagement.

There is currently one Topical Requirement, Cybersecurity, released in February 2025. The IIA has indicated future Topical Requirements may address:

- Third-party
- Culture
- Business resiliency

3 Scope

After establishing engagement objectives, the engagement scope is determined. Determining the scope relies on applying professional judgment to consider each objective independently, ensuring it can be accomplished by the engagement.

The scope should be sufficiently broad to achieve all engagement objectives. The engagement scope is documented in an approved engagement work program, which specifically identifies what is included or excluded in the engagement. Minutes from meetings with stakeholders where the scope was discussed should also be retained.

Relevant systems, records, personnel, and physical properties should all be considered when establishing scope. Scope statements may lay out the following:

- Boundaries of the process
- In-scope and out-of-scope locations
- Related subprocesses or components of processes
- Time frame

Pass Key

The scope of the engagement identifies what is included in the engagement and what is excluded from the engagement.

© Becker Professional Education Corporation. All rights reserved.

Illustration 2 Example Scope Statements

- This engagement will focus on the accounts payable function's compliance with the organization's payables policies. All clinic locations in the southeast operating region will be included, considering all accruals and disbursements from Q4 (October 1–December 31).
- The audit will assess IT network security controls at the corporate level, including access and privilege management protocols, data collection and protection, firewall protections, and incident responses for the period of January 1 to June 30.
- This engagement will examine the organization's accounts receivable aging process to ensure compliance with U.S. GAAP and will include allowance recording, monitoring, write-offs, and documentation for all mills except one location during Q3 (July 1–September 30). The one location will be excluded because of a recent comprehensive review performed at this mill.
- The audit will evaluate fraud risk management practices, focusing on fraud prevention, including controls related to cash handling at all individual retail outlets grossing greater than $2M during the month of November.

3.1 Scope Limitations

Scope limitations are conditions that prevent internal auditors from performing work as intended, such as:

- Resource constraints.
- Restrictions on access to personnel, facilities, data, and information.
- Stakeholder requests for items to be included in or excluded from the scope.
- A restriction on the length of the engagement.

When a scope limitation arises in an engagement, it should be documented, and internal auditors should attempt to achieve a resolution with management. If they are unable to do so favorably, the chief audit executive (CAE) must raise the issue to the board, including discussion of the implications, according to an established methodology.

© Becker Professional Education Corporation. All rights reserved.

Illustration 3 Scope Limitations

In June, the internal audit function began a comprehensive assessment of data transmission controls for the galvanizing divisions of an organization of steel mills. The organization practices extreme decentralization, and there are no standard IT systems and data transmission practices across mills.

The galvanizing division manager of one location reached out to the CAE with concerns about the ongoing audit. After committing to the planned timeline and audit plan, the manager recalled that the mill will update the enterprise resource planning system to the latest version during some of the scheduled fieldwork. The update must be completed now to ensure continuity in production; therefore, the assessment of data transmission controls must be delayed until some point in the future.

This constitutes a scope limitation. If the CAE is unable to persuade the manager to let the audit work continue, the interference must be documented and reported to the board, along with a discussion of the implications.

4 Changes in Objectives and Scope

4.1 Evaluating and Documenting Stakeholder Requests

Part of the responsibilities of the internal audit function is to manage stakeholder requests. The CAE, board (governing body), and senior management should meet regularly to discuss expectations for the internal audit function, which will influence and be documented in the internal audit charter, internal audit mandate, and internal audit plan.

When internal auditors begin an engagement, they should understand any stakeholder expectations that exist regarding the purpose, objectives, and scope of the engagement. Expectations may differ based on whether it is an assurance or advisory (consulting) engagement.

If the objectives or scope change, stakeholders should be timely notified to help manage their expectations and the reasons for the changes documented.

4.2 Addressing Changes in Objectives and Scope

Throughout an engagement, internal auditors may obtain information, or audit work may identify that the objectives and scope need to be changed. For example, internal auditors may learn that an in-scope retail outlet of the organization is closing in the next three months. The inclusion of this location may no longer add value.

Effective methods for addressing the changes include communication with the board, senior management, and stakeholders, as well as sufficient documentation of the changes and rationale.

The CAE must approve any changes in scope or objectives that occur during the engagement. In some cases, the engagement scope may need to be expanded to address engagement objectives appropriately.

© Becker Professional Education Corporation. All rights reserved.

5 Deliverables and Communication

After establishing objectives and determining the engagement scope, internal auditors should consider potential testing outcomes and engagement communications. Testing could result in the discovery of financial statement errors, control deficiencies, failure to achieve engagement objectives, inefficiencies, or instances of noncompliance. Anticipating these possibilities can assist internal auditors with establishing clear and appropriate objectives.

Common types of communication include full-scope internal reports for wide distribution, internal reports with limited distribution, reports to third parties, or confidential reports. Understanding the types of communication relevant to the engagement can assist internal auditors in preparing the objectives, determining the scope, and ensuring all necessary evidence is obtained during the engagement.

Common engagement deliverables evidencing objectives and scope include the engagement planning memorandum and workpapers documenting:

- the alignment of objectives to risk assessments;
- how the scope achieves objectives;
- the relevant work programs;
- any minutes from stakeholder meetings about objectives and scope;
- any scope limitations or relevant stakeholder requests, along with their related resolutions; and
- final engagement communication.

6 Identifying Relevant Criteria

Requirements **Standard 13.4 Evaluation Criteria**

Internal auditors must identify the most relevant criteria to be used to evaluate the aspects of the activity under review defined in the engagement objectives and scope. For advisory services, the identification of evaluation criteria may not be necessary, depending on the agreement with relevant stakeholders.

Internal auditors must assess the extent to which the board and senior management have established adequate criteria to determine whether the activity under review has accomplished its objectives and goals. If such criteria are adequate, internal auditors must use them for the evaluation. If the criteria are inadequate, internal auditors must identify appropriate criteria through discussion with the board and/or senior management.

Evaluation criteria represent the desired state of an activity under review that internal auditors compare with the existing state of an activity (i.e., the criteria by which internal auditors evaluate the activity's condition) and should be specific and practical.

© Becker Professional Education Corporation. All rights reserved.

The board (governing body) and senior management often have established criteria, which internal auditors identify during information gathering and while planning the engagement. Internal auditors can compare the established criteria to those of other organizations, recommended industry practices, and use professional judgment to determine whether the criteria are relevant and the best for achieving the engagement objectives.

Internal auditors should look to the engagement objectives to help identify the most relevant criteria that will help in preparing meaningful engagement conclusions. An example provided in the Standards explains that "if an engagement objective is to assess the effectiveness of the control processes in the activity under review, the criteria could be the expected results or outcomes of the activity's control processes, while the condition is revealed by the actual outcomes."

Ultimately, the most relevant criteria should be used in the engagement to align with organizational objectives and the activity under review. Internal auditors may offer suggestions for other or better engagement criteria, assist in identifying relevant criteria, and/or use experts to help identify and develop relevant criteria.

Examples of adequate criteria provided in the Standards include:

- Internal (e.g., policies and procedures of the organization, key performance indicators, or targets for the activity).
- External (e.g., laws and regulations imposed by statutory bodies and contractual obligations).
- Authoritative guidance (e.g., frameworks, standards, guidance, and benchmarks specific to an industry, activity, or profession).
- Established organizational practices.
- Expectations based on the design of a control.
- Procedures that may not be formally documented.

Example 1 Types of Criteria

The following represent example types and sources of criteria. The adequacy and relevance of these depend on the actual objectives of the activity. Best practices and standards for criteria are established by professional associations (e.g., COBIT from ISACA):

- Industry journal articles about Six Sigma quality initiatives
- Scholarly texts about logistics' supply chain practices
- Benchmarks for marketing functions
- Historical data about waste and scrap materials
- IRS requirements around W2s
- Employee job satisfaction levels
- Corporate P-Card internal use policies

© Becker Professional Education Corporation. All rights reserved.

Whatever type of criteria is chosen, it must be specific enough to be useful to the client. As directed by the Standards, "Internal auditors should inform the management of the activity under review of the criteria to be used during the engagement." Once established and agreed upon, the evaluation criteria should be documented to avoid misinterpretation. The Standards recommend that internal auditors maintain the documentation (meeting minutes, planning memorandum, or email) of the discussions with the board, senior management, and management of the activity under review regarding the criteria.

Pass Key

Evaluation criteria that are most relevant to the engagement represent the desired state of the activity under review and should be specific and practical (e.g., the expected results or outcomes of a process).

6.1 Advisory Engagements

In advisory engagements, engagement objectives, as well as the criteria used to evaluate whether the objectives are met, depend on agreement with the client. In some cases, the identification of criteria may not be necessary.

7 Assessing Evaluation Criteria

Internal auditors must determine whether the evaluation criteria are adequate to determine whether the activity under review has accomplished its objectives and goals and will help in determining the significance of findings.

Internal auditors use professional judgment to determine whether the organization's criteria are adequate, which includes assessing whether the criteria are:

S: **S**pecific—the criteria should be specific enough to determine whether the desired state of the activity has been achieved.

C: Produce Reliable **C**omparisons—the criteria should be able to consistently produce "apples to apples" comparisons of the audit activity.

R: **R**elevant—the criteria must actually relate to the objective being tested.

A: **A**ligned—criteria should be aligned with the objectives of the organization and the activity under review in order to be useful.

P: **P**ractical—the criteria should be practically observable through planned procedures to evaluate the activity.

Adequate criteria should be measurable, as it will serve as a benchmark for the subject matter assessed in the engagement. Without adequate criteria, internal auditors cannot determine the significance of findings or conclude reasonably in an assurance engagement.

© Becker Professional Education Corporation. All rights reserved.

When evaluating criteria adequacy, the Standards indicate that internal auditors should consider:

- the organization's basic principles to define appropriate governance, risk management, and control processes;
- the organization's established risk tolerance, including materiality thresholds for various business units, functions, or processes; and
- the level of control adopted and whether it is satisfactory (e.g., satisfactory could mean that a certain percentage of transactions within one control objective are conducted in accordance with established control procedures or that a certain percentage of controls overall are working as intended).

If internal auditors determine that management's evaluation criteria are inadequate, internal auditors should establish the most appropriate criteria for their evaluation. Additionally, when there are inadequate criteria or no criteria exist, this may create an opportunity for the internal audit function to perform an advisory engagement.

Internal auditors should document the sources of criteria and the process used to determine the adequacy of the criteria in the workpapers.

Pass Key

Consider the mnemonic **SCRAP** to help in remembering the considerations when evaluating criteria adequacy:

S: **S**pecific

C: Produce Reliable **C**omparisons

R: **R**elevant

A: **A**ligned

P: **P**ractical

© Becker Professional Education Corporation. All rights reserved.

MODULE

2 Topical Requirements and Strategic Objectives

Part 2
Unit 1

This module covers the following topics from the *CIA examination syllabus*:

CIA Syllabus—Section A: Engagement Planning

3. Plan the engagement to assess key risks and controls

   May include but is not limited to:

   a. Recognize how to apply Topical Requirements when planning an engagement

   b. When planning an engagement, recognize the strategic objectives of the activity under review and their integration with risk management, business performance measures, and performance management techniques

1 Understand the Activity Under Review When Planning

Requirements **Standard 13.2 Engagement Risk Assessment (Excerpt)**

Internal auditors must develop an understanding of the activity under review to assess the relevant risks. For advisory services, a formal, documented risk assessment may not be necessary, depending on the agreement with relevant stakeholders.

To develop an adequate understanding, internal auditors must identify and gather reliable, relevant, and sufficient information regarding:

- The organization's strategies, objectives, and risks relevant to the activity under review.
- The organization's risk tolerance, if established.
- The risk assessment supporting the internal audit plan.
- The governance, risk management, and control processes of the activity under review.
- Applicable frameworks, guidance, and other criteria that can be used to evaluate the effectiveness of those processes.

Internal auditors must review the gathered information to understand how processes are intended to operate.

© Becker Professional Education Corporation. All rights reserved.

Obtaining a comprehensive understanding of the activity under review is a crucial part of engagement planning. This includes recognizing the activity's strategic objectives and their integration with risk management, performance measures, and management techniques. It also involves understanding information technology, cybersecurity, and data-related risks. Furthermore, it necessitates recognizing business continuity and disaster recovery concepts, relevant finance and accounting concepts, and key risks and controls related to common business processes. Failure to understand the activity under review is likely to weaken the value and relevance of the engagement and may lead to incomplete testing plans or the misallocation of internal audit resources.

1.1 Understanding Strategic Objectives

The first step in understanding the activity under review is to identify the key strategic objectives. This allows internal auditors to gain insights into why the activity and related processes exist, facilitating the next steps of identifying and evaluating key risks and controls related to those objectives. Risk is the effect of uncertainty on objectives.

1.1.1 Identifying Objectives

Strategic objectives of the activity under review are established by management to align with the organizational objectives and goals. The organizational objectives define the purpose for processes and link daily operations to the achievement of organizational objectives. Such objectives may include:

- Objectives to achieve operational effectiveness and efficiency.
- Objectives to meet internal and external reporting requirements.
- Objectives to conform with external laws and regulations and internal policies and procedures.
- Objectives related to specific processes or initiatives.

1.1.2 Collection of Relevant Information

Internal auditors may obtain a list of strategic objectives from the process owner or the individual responsible for the activity under review. In cases where written objectives are not available, internal auditors should have discussions with management to understand what management wants to accomplish.

Additionally, internal auditors may review relevant documents about the activity under review to identify its objectives. These may include:

- **Business or Operating Plan:** Gain insights into the strategies adopted by the activity under review to achieve its purposes/objectives.
- **Measures and Metrics:** Understand how progress is tracked and performance is measured.
- **Organization Chart:** Review the overall structure to understand how people and functions are interrelated and identify individuals responsible for particular processes.
- **Process Maps, Risk/Control Matrices, or Process Narratives:** Obtain an overview of the processes and their operations.
- **Job Descriptions:** Understand the details of employees' responsibilities.
- **Key Policies:** Understand the principles guiding decisions and actions.

© Becker Professional Education Corporation. All rights reserved.

1.2 Integration of Strategic Objectives With Risk Management

Internal auditors should gain an understanding of how management integrates strategic objectives with risk management at the organization, which aligns well with the strategy and objective-setting component in COSO's *Enterprise Risk Management—Integrated Framework.* This component involves management incorporating risk considerations into every stage of the strategic planning process. It starts with analyzing the broader business environment to understand how external and internal factors could influence the organization's risk profile. This analysis helps define the organization's risk appetite, ensuring its alignment with the goals of creating, preserving, and realizing value for the organization.

When exploring different strategies, the organization evaluates them for their potential to achieve strategic objectives, as well as for their impact on the organization's risk profile. In setting strategic objectives at various levels, the organization needs to consider associated risks and ensure that these objectives are formulated to align with broader strategies at the organizational level.

1.3 Integration of Strategic Objectives With Performance Measurement and Management

Internal auditors need to understand how performance is measured and managed for the activity under review since performance measures are crucial for the achievement of strategic objectives. Internal auditors review and evaluate the reasonableness, reliability, efficiency, and effectiveness of these measures and management techniques.

1.3.1 Performance Measures

A robust performance measurement system involves establishing performance targets, determining associated metrics to measure performance, communicating these measurements and targets to responsible persons or entities, monitoring performance against targets, and following up on variances to take corrective actions as needed. The organization and each business function should have a set of key performance measures to evaluate outcomes and key performance indicators to help assess how the organization or function is performing and whether it is on the right track.

- **Key Performance Indicators (KPIs)**

  KPIs are high-level metrics that provide a summary of key accomplishments or behaviors valued by the organization or business function to meet its objectives. They are used to track the organization's or business function's progress toward its goals. There are generally two types of KPIs:

  - Quantitative KPIs using numerical measures (e.g., sales figures, customer retention rate)
  - Qualitative KPIs based on quality or performance (e.g., product quality, employee morale)

  For KPIs to be effective, they need to measure relevant aspects, provide useful information to management, and guide improvements in key strategic areas.

- **Key Risk Indicators (KRIs)**

  Organizations with a mature Enterprise Risk Management function might use KRIs to monitor critical objectives, operations, and processes. KRIs are metrics that provide early warnings of increasing risks in specific areas. They are often used as leading indicators, which are measures used to predict performance based on process inputs. They complement lagging indicators that confirm past performance by measuring outputs. When a KRI shows a worrying trend or crosses a set threshold, management can address the root cause early and take corrective action before any significant damage is done.

© Becker Professional Education Corporation. All rights reserved.

- **Considerations in Measuring Performance**

  As well as monitoring performance, management should routinely evaluate the effectiveness and efficiency of the performance management system. Monitoring performance metrics is an essential oversight responsibility of management. Management needs to evaluate the performance measurement system to determine its effectiveness in indicating whether organizational objectives are being achieved, as well as its efficiency in cost allocation relative to value creation. For instance, while too few KPIs might imply a lack of incentive to pursue some of the organization's or business function's objectives, too many KPIs may cause information overload and incur excessive administrative costs.

  The following steps can be taken to measure the performance of the organization or business function:

  - **Step 1:** Identifying performance targets, including internal targets to achieve organizational or functional objectives and external targets required by laws and regulations.
  - **Step 2:** Evaluating the reasonableness of performance targets and measurement metrics in accomplishing the objectives of the organization or business function.
  - **Step 3:** Assessing the reliability, efficiency, and effectiveness of the inputs (e.g., data), processes (e.g., the error correction process), and outputs (e.g., timeliness of updates).
  - **Step 4:** Comparing performance against established performance targets.
  - **Step 5:** Determining performance gaps (i.e., variances from targets).
  - **Step 6:** Identifying corrective actions and following up on their implementation.

1.3.2 Assessing Performance Measures

To evaluate the design of performance measures of the activity under review during engagement planning, internal auditors may consider the following factors:

- **Appropriateness:** Are they the right indicators to use?
- **Accuracy:** Do they correctly indicate how the organization or business function is performing in achieving objectives?
- **Completeness:** Do they incorporate everything that needs to be considered?
- **Reliability:** Are the data inputs from reliable sources?
- **Understandability:** Can internal and external stakeholders understand them clearly?
- **Timeliness:** Are they timely in providing outcomes of the performance?

When assessing the effectiveness and efficiency of KPIs and performance management systems, internal auditors also need to consider the following specific questions:

- **KPI Design Effectiveness:** Do the KPIs cover all the objectives? Do they ensure that objectives of higher importance get sufficiently prioritized? Do they consider other priorities to the extent possible while remaining efficient?
- **KPI Operation Effectiveness:** Are the calculations accurate? Are errors uncovered and corrected in time? Do they result in positive changes in actual performance?
- **KPI Operation Efficiency:** Are there the right number of KPIs for timely decision making? Can the data be collected, prepared, and analyzed in a timely and cost-effective manner? Are the reports or analyses ready by the time decisions need to be made?

© Becker Professional Education Corporation. All rights reserved.

1.3.3 Balanced Scorecard

The balanced scorecard gathers information on multiple dimensions of an organization's performance, as defined by the critical success factors (the critical elements an organization must focus on to achieve its strategic objectives) necessary for the organization to accomplish its mission. It includes nonfinancial and financial information and analyzes information from the following four perspectives: financial, customer, internal processes, and learning and growth. The components of the balanced scorecard include:

- **Financial Measures:** Includes return on assets (ROA), return on investment (ROI), profit margins, asset turnover ratios, and other traditional ratio measures used by managers.
- **Internal Business Processes:** Nonfinancial measures such as quality and efficiency of the organization's performance related to its products and services.
- **Customer Satisfaction:** Nonfinancial measures, including customer retention and number of customer repeat visits.
- **Learning and Growth:** Nonfinancial measures that focus on the human resources of the organization.

The learning and growth perspective is seen by many as the most important. A satisfied employee may be more innovative and may engage in developing internal processes and products, which will lead to customer satisfaction. Satisfied customers help the organization achieve its financial goals.

Typically, the scorecard describes the classifications of critical success factors, the strategic goals, the tactics (how to achieve the goals), and the related measures associated with the strategic goals and tactics.

- The strategy of the organization must be the core of a balanced scorecard.
- The number of measures must be limited, identifying those that are most crucial (such as the key performance indicators).
- Short-term and long-term objectives must be balanced. For example, reducing R&D will lead to higher profits in the short run but could negatively affect long-term objectives.

Illustration 1 Balanced Scorecard

A manufacturing company is building its business using a cost leadership strategy. Management has identified four strategic goals, one associated with each classification of critical success factors, to help its business grow. The strategic goals are:

1. Capturing additional market share
2. Maintaining low costs that are supported by low prices
3. Becoming a low-price leader
4. Linking strategy with reward and recognition

The company should design tactics to achieve its strategic goals, define measures it might use, and organize them in the manner of a balanced scorecard.

© Becker Professional Education Corporation. All rights reserved.

(continued)

	Tactics	Measures
Financial Perspective		
Strategic goals	Capture increasing market share	Company vs. industry growth
Critical success factors	Maintain customer base	Volume trend line
Tactics and measures	Steadily expand services	Percentage of sales from new products
Internal Business Processes		
Strategic goals	Maintain low costs that are supported by low prices	Costs compared to competitor
Critical success factors	Maintain consistent production	First pass rates
Tactics and measures	Improve distribution efficiency	Percentage of perfect orders
Customer Perspective		
Strategic goals	Become a low-price leader	Our cost vs. competition
Critical success factors	Anticipate customer needs before competitors	Percentage of products in R&D being test-marketed
Tactics and measures	Increase customer satisfaction	Customer surveys
Advance Learning and Innovation (Human Resources)		
Strategic goals	Link strategy with reward and recognition	Net income per dollar of variable pay
Tactics and measures	Promote entrepreneurial culture	Annual reports

Now that the various tactics and measures have been defined, management should set benchmark values for each measure and then compare actual results with benchmark values. Management should also periodically review the chosen measures to ensure that they continue to represent the established goals and tactics accurately.

1.3.4 Performance Management Techniques

Techniques that management may adopt to manage employee performance include daily management interaction with subordinates, workgroup design, job design, rewards, and performance appraisals. With a comprehensive understanding of the organizational environment and culture, management can effectively apply appropriate performance management techniques to minimize organizational risks. Management and internal auditors can also assess these techniques for their effectiveness.

- **Interaction With Employees**

  Managers and supervisors interact with employees on a regular basis, making the relationships between managers, supervisors, and employees key to workplace attitudes and employee retention. When managers set high but achievable expectations and foster a positive environment, employees are more likely to succeed. Providing clear goals, resources, and constructive feedback helps employees meet expectations.

© Becker Professional Education Corporation. All rights reserved.

Managers should understand how to apply motivational theories in the workplace. Trust is built by delegating to responsible employees and expressing confidence in their abilities, which boosts morale and empowers teams. Regular and constructive feedback is also crucial in motivating employees, as feedback is helpful for employees' growth.

- **Work Group Design**

  Employees' attitudes and behaviors are affected by how their work is organized. Organizations commonly use teams and work groups to achieve goals, with rewards tied to team outcomes. Teams and work groups also fulfill employees' social and affiliation needs at work. Designing work groups involves determining team composition, setting goals, and establishing rules for interacting with managers, team members, and other stakeholders. Including team members in the design process can increase their engagement and commitment.

- **Job Design**

  How a job and its tasks are designed and organized influences employee attitudes and behaviors. Job design involves determining job tasks, the order in which tasks are performed, the way they are performed, and their relation to other jobs in the organization. Job design should also be reviewed and adjusted over time, as needed, to ensure relevance and boost employee morale. These adjustments may include:

  - Job enlargement to broaden the scope of a job with similar or different tasks, which may reduce the risk of boredom and encourage employees to learn, although their responsibilities may not necessarily be increased.
  - Job rotation, during which employees move between different tasks and jobs, becoming cross-trained.
  - Job enrichment when more responsibilities are added to a job, increasing employees' engagement, accountability, and independence.

- **Reward System Design**

  Both intrinsic (originating internally within an individual) and extrinsic (originating externally) rewards have an impact on employee behavior. To develop an effective reward system, management may consider the following factors:

  - Offer rewards that are meaningful to employees and will have a lasting impact.
  - Match rewards to the level of achievement.
  - Ensure rewards are readily available for distribution and are delivered promptly after accomplishments.
  - Effectively communicate the reward system to all employees and clearly explain the reasons behind the determination of individual or team rewards.
  - Establish equitable policies that align with internal and external standards.
  - Praise publicly, but distribute rewards privately to minimize perceptions of unfairness.

- **Performance Appraisals**

  Performance appraisals are used to link job performance to the reward system. Following a formal process, they are traditionally conducted on a set schedule. It is becoming more common to prioritize more frequent performance feedback. Regardless of the methodology, the focus of performance appraisals should be aimed at achieving efficient communication between managers and employees, facilitating employee development and growth. Additionally, input from other sources can also be incorporated into the appraisal process, including feedback from the employee's peers, customers, the employee themselves, or a combination of all (e.g., a 360-degree performance evaluation).

© Becker Professional Education Corporation. All rights reserved.

2 Identifying Key Risks and Controls

2.1 Identifying Key Risks

After developing an understanding of the processes of the activity under review, internal auditors are required to assess key risks and the associated controls to mitigate these risks. Since risks exist in all processes, the first step when assessing process-level risks is to identify inherent risk scenarios that may affect objective achievements.

2.1.1 Identifying Risk Scenarios

Brainstorm sessions can be conducted to identify potential risk scenarios. To maximize the output from these sessions, internal auditors may consider inviting personnel involved in the process to participate. The brainstorming session can be conducted by following these steps:

- Focus on one process-level objective at a time.
- Brainstorm barriers or missed opportunities that might hinder objective achievement, such as failure to measure performance appropriately, inadequately designed technology applications, or inaccurate or untimely information for decision making.
- Continue the exercise for the remaining process-level objectives.
- Categorize and combine similar risk scenarios to facilitate process-level risk identification.

2.1.2 Defining Process-Level Risks

Using a "cause and effect" protocol is a common and effective approach for defining process-level risks. The exercise starts with finding a "cause" (e.g., lack of ... , failure to ...) and then determining the "effect" (e.g., financial loss, data corruption). Below are some examples:

- Lack of effective logical security controls may lead to unauthorized access, manipulation, or deletion of data.
- Failure to attract, develop, and retain competent individuals may result in inappropriate handling of certain tasks, potentially damaging the proper functioning of the process.
- The inability to process payments on time may cause penalties for late payments.

Once the risks are identified, using brainstorming or another method, internal auditors should link them to process-level objectives and then evaluate the likelihood and impact of these risks on the ability to achieve objectives during the risk assessment process. The outcome of the risk assessment serves as a foundation for identifying controls that could mitigate key risks.

2.2 Identifying Key Controls

Key controls are designed to address risks associated with critical business objectives. Identifying key controls requires internal auditors' judgment and can be achieved by answering this question: If not performed as designed, which of these controls would likely result in the inability to achieve the process-level objectives?

© Becker Professional Education Corporation. All rights reserved.

Controls that mitigate relevant risks are likely to be key controls. Internal auditors should consider the following when determining key controls:

- Obtain a clear understanding of the process-level objectives.
- Evaluate the consequences of inadequate control execution to determine whether a control deficiency would significantly impair objective achievement.
- Consider other compensating controls to determine whether the operation of a given key control is as critical as presumed.
- Consider the impact of one control on other controls, especially when the execution of one control influences the execution of other controls.
- Consider the effect of entity-level controls on process-level controls, especially when deficiencies in entity-level controls may reduce the effectiveness of process-level controls.
- Consider redundant or less cost-effective controls, which may be changed or eliminated.

Once the controls are identified, they should be linked to process-level risks. The documentation of such a linkage can be achieved by using a risk and control matrix.

3 Applying Topical Requirements in Engagement Planning

Topical Requirements are one of the components of the International Professional Practices Framework® (IPPF), which also includes the *Global Internal Audit Standards*. When an internal audit function provides assurance on a specific risk area covered under Topical Requirements, internal auditors must follow these requirements, including applying them during engagement planning. Areas covered under Topical Requirements include (or will include) cybersecurity, culture, third-party, and business resiliency.

Topical Requirements include the following elements:

- Mandatory requirements for the evaluation of governance, risk management, and control processes
- Nonmandatory considerations facilitating internal auditors' implementation of mandatory requirements

The applicability of Topical Requirements is determined by the risk-based internal audit plan, with any limitations in scope being clearly documented. When a risk area is under review, Topical Requirements serve as the baseline for evaluating engagement performance and are also subject to external quality assessment.

© Becker Professional Education Corporation. All rights reserved.

NOTES

© Becker Professional Education Corporation. All rights reserved.

MODULE

3 IT Considerations

Part 2
Unit 1

This module covers the following topics from the *CIA examination syllabus*:

CIA Syllabus—Section A: Engagement Planning
3. Plan the engagement to assess key risks and controls *May include but is not limited to:* c. When planning an engagement, recognize existing and emerging cybersecurity risks, common information security and IT controls, IT general controls, the purpose and benefits of using an IT control framework, principles of data privacy, and data security policies and practices

1 Assessing Key IT Risks and Controls During Engagement Planning

Requirements **Standard 13.2 Engagement Risk Assessment (Excerpt)**

Internal auditors must develop an understanding of the activity under review to assess the relevant risks. For advisory services, a formal, documented risk assessment may not be necessary, depending on the agreement with relevant stakeholders.

Internal auditors must identify the risks to review by:

- Identifying the potentially significant risks to the objectives of the activity under review.
- Considering specific risks related to fraud.
- Evaluating the significance of the risks and prioritizing them for review.

As part of engagement risk assessment during planning, internal auditors identify risks and controls related to the engagement objectives of the activity under review. IT risks and controls can impact many business processes within an organization. IT risks and controls may include:

- Cybersecurity risks, including data security risks and controls.
- Information security and IT controls.
- IT general controls.

© Becker Professional Education Corporation. All rights reserved.

As with other risks and controls, the IT-related risks and controls should be documented, and the significance of the risks should be assessed using the internal audit team's knowledge, experience, and critical thinking to make judgments regarding significance, which is used for prioritization.

Input from management of the activity under review should be considered in the understanding of the risks and controls. Additionally, an internal auditor should reference other sources available to assist with understanding and identifying emerging IT risks. For example, The IIA's *Cybersecurity Topical Requirement* provides a consistent, comprehensive approach to assessing the design and implementation of cybersecurity governance, risk management, and control processes. As the engagement progresses, additional information, including the type of control (preventive, detective, directive, or corrective), is determined and documented as part of the engagement.

Factors for internal auditors to consider when assessing IT risks and controls include:

- The complexity of the IT infrastructure and environment.
- Appropriateness of IT controls.
- Providers of IT systems and controls (internally developed or external).

1.1 Identifying IT Risks and Controls

Understanding the organization's IT infrastructure, including its components (hardware, software, network, and data components) and environment, helps to identify potential IT-related risks for the organization. Internal auditors should also understand the IT strategy and processes to help identify the IT-related risks at the organization and within the process or scope of the engagement.

The CAE should discuss the IT risks with the CIO and process owners. The Standards outline that internal auditors should review risk assessments recently conducted by the internal audit function, management, or external service providers. The identification of risks should also include the existence of controls to mitigate the risks.

Many models and approaches can be used to identify and assess IT risks, including considering them in layers to help understand the audit priority, risk assessment, and control evaluation. The IT management layers include IT management, external connections (internet, customers, and vendors), technical infrastructure, and applications (software).

Internal auditors should consider leveraging an IT control framework, such as COBIT, that is used by the organization in the risk assessment to help ensure IT-related risks are considered appropriately. If the organization does not use an IT control framework, the CAE should select an appropriate framework.

1.2 Assessing IT Risks and Controls

As with other risks, part of the risk assessment process for IT-related risks includes assessing the likelihood and magnitude of the impact of risks on the process and/or organization and what controls, if any, exist to help mitigate these risks. The risks are then assessed based on the risk appetite and tolerance of the organization to help in the prioritization of risks during planning.

It may also be helpful to group IT risks and controls to help with identifying and allocating appropriate internal auditors with the necessary knowledge and skills to those areas.

© Becker Professional Education Corporation. All rights reserved.

2 Information Security

Understanding information security is part of the technical infrastructure IT management layer and is key in the planning and risk assessment for engagements impacted by IT-related risks. Information security involves policies, processes, and procedures to protect an organization's intellectual property by maintaining the confidentiality, integrity, and availability of its data, regardless of format (electronic, print, or other).

Information security includes setting up appropriate controls, as well as continuously monitoring and responding to security threats. Risks and controls related to information security can apply to data in storage, processing, and transit.

2.1 Information System Security Controls

Common information security controls relating to access to data include log-in credentials. Controls relating to preventing changes to programs and databases also include version controls, access controls, and validity controls.

To help protect programs and databases from unauthorized use, access to data in a system is always linked to each employee's log-in credentials. This allows IT to set limits on each employee's ability to use any part of a program. Such programs also keep records of every action taken and link those actions to the employee who performed the action.

In addition to log-in credentials, programs and databases have protocols that prevent changes to the program or database unless each part of the change adheres to internal rules, including:

- **Version Controls:** Allow only one change at a time, incorporating all users' changes in a sequential manner so that no content is overwritten or lost.
- **Access Controls:** Allow only authorized users to make changes.
- **Validity Controls:** Allow only data types that meet certain parameters (such as being numerical or within a specified range) and may restrict the relationship with other data points after changes are made.

2.2 Physical Systems Security Controls

Computer software and hardware, including peripheral devices, require preventive controls over physical systems.

- Computers at customer-serving offices should be secured with log-in credentials, as well as secured against being physically stolen. For this reason, the computer that controls a point-of-sale system is kept in a locked location with a small opening for wires to reach a screen and a keyboard.
- Other employee-use computers should be behind a locked door in a restricted-access area for employees only.
- Computer servers should also be stored in locked rooms, accessible only by authorized employees. This control exists to prevent anyone without authorized credentials from accessing, stealing, altering, or destroying sensitive organizational data by either stealing a hard drive or destroying a server. Another physical security feature in a server room is a lack of physical labeling. An unauthorized individual would have a difficult time searching for a particular set of files or data to steal in a server room where every server is essentially physically identical.

© Becker Professional Education Corporation. All rights reserved.

- Peripheral devices may create vulnerabilities that are just as significant as exposed core hardware and software. They could be assets that allow indirect access to core systems, such as an IoT (Internet of Things) piece of equipment. Or peripheral devices could be more supportive in nature, particularly central heating and cooling systems, which are critical to maintaining low-temperature levels for servers, switches, and other items found in a data center. Access to central cooling systems that support such equipment should be given the same level of physical access controls because tampering with it could be just as detrimental, potentially causing equipment to overheat.

2.3 Risks and Threats to Information System Security

Risks may also be identified that are part of the external connections IT management layer. External parties, such as contractors, cloud service providers, customers, vendors, competitors, and hackers, may gain access to an organization's data. These external parties gain access by attacking the organization's people and systems in a variety of ways, including:

- **Phishing:** A form of digital social engineering that uses authentic-looking (but fake) emails that request information from users or direct them to a fake website that requests information.
- **Trojan Horse:** An apparently benign program or application that executes a malicious script or program in an attempt to capture a user's credentials, steal data from the computer, alter files, or cause destruction to the computer's software and operating system.
- **Ransomware:** Encryption of data files by an attacker that requires victims to pay in order to receive a decryption key to recover the data.
- **Viruses:** A malicious code that attaches itself to storage media, documents, or executable files and is spread when the files are shared with others.

Once an attacker has access to the system, the attacker may attempt to copy, steal, deny access, alter, or destroy input data files. An attacker who seeks to sell data or ransom it back to the organization may attempt to copy, steal, or deny access to the data; someone who is either a former disgruntled employee or engaging in corporate espionage may be more likely to alter or destroy files or systems.

Other threats to information systems include input manipulation, program alteration, direct file alteration, data theft, and sabotage. Criminals may profit from their actions by adding programs to fraudulently divert profits into their personal accounts or to disrupt the targeted organization for pay offered by a competitor.

2.4 Internet Security Risks and Controls

Using the internet is inherently riskier than transmitting data over secured transmission lines because the internet routes data transmissions through unpredictable paths. Even if data is sent from one company-owned computer to another company-owned computer, that data may circulate to other computers outside of the originating company's network.

Security safeguards along this path may vary widely, so sensitive data should be encrypted to protect it from unauthorized copying or altering as the data flows throughout this channel. These issues are further complicated if the data is exposed to wireless networks during any of these steps along the path because they have notoriously weak security systems in place, making such copying significantly easier.

© Becker Professional Education Corporation. All rights reserved.

2.5 Encryption

Encryption is a preventive control that is used to protect data. There are various types of encryption mechanisms, but the most basic types of encryption involve the use of a computer algorithm to transform data from a readable state into an unreadable state in a process called encoding. The encryption program is designed to prevent unintended access by use of one or multiple encryption keys. The decryption key is typically a string of characters that serve as input parameters to unlock or undo the encryption. An encryption key can also be thought of as a set of instructions that the program needs to undo the initial encoding that it performed, returning the data to its original state.

Data encryption is particularly important when using the internet because of the type of data being exchanged. Financial services companies and banks transmit personal account numbers. Healthcare institutions swap sensitive medical data and other personally identifiable information, such as Social Security numbers or demographic data. Other organizations that do not deal directly with personal health or financial information may store payment data for future transactions, such as online retailers that accept payment from credit cards. The use of encryption for transactions and data storage adds a layer of protection for all parties involved.

2.6 Firewalls

Another common type of information system security control is a firewall. Firewalls are network security systems that are intended to protect an organization by monitoring, controlling, and restricting incoming and outgoing traffic. Firewalls are used to selectively allow or deny communications traffic based on a set of predetermined rules designed by organization administrators. Firewalls may deny access based on port or the Internet Protocol (IP) address of the incoming communication, which can be as macro-focused as excluding nations or regions, or as micro-focused as excluding organizations or individuals.

Firewalls can deny access depending on which programs are used for the communication. This type of restriction is often used to block communications that contain executable code attached to the message. Firewalls may be used to deny use or filter types of internet content. For example, websites tagged as gaming or adult are frequently blocked by employers. Additionally, a firewall may be set up on a default-allow policy (in which traffic is allowed unless specifically excluded) or a default-deny policy (traffic is only allowed from specifically identified sites).

Pass Key

Two similar controls are data encryption and data decryption.

- Data encryption is turning plain text into cyphertext.
- Data decryption is turning cyphertext back into plain text.

© Becker Professional Education Corporation. All rights reserved.

3 Cybersecurity Risks

3.1 Overview

Cybersecurity is the practice of protecting an organization's IT infrastructure and critical data from bad actors by deploying a variety of technologies, internal control processes, and best practices to mitigate the business impact of cyberattacks. The goal of a cybersecurity program is to manage cybersecurity risks by securing and enhancing confidentiality, data integrity, and availability.

A cyber threat is an action by an external or internal party using an information system to compromise the organization's information assets (steal, destroy, or alter data). Types of cyber threats vary by industry and organization. The activity that is performed is referred to as a cyberattack.

Successful cyberattacks can create both monetary and nonmonetary losses for the organization as they restrict the ability to work with customers, vendors, and partner organizations.

These attacks are threats to both individuals and organizations. Breaches of data, theft, service interruptions, and regulatory noncompliance are the highest security concerns for senior executives and others who are charged with IT governance.

3.2 Identifying and Assessing Cybersecurity Risks

As described in The IIA's Global Technology Audit Guide: "Assessing Cybersecurity Risk, The Three Lines Model," published in 2020, cybersecurity risks can be identified and assessed by considering:

- Who has access to the data.
- Likely targets for cyberattacks.
- Systems that would cause the most significant disruption if compromised.
- Which data would result in financial or competitive loss, legal ramifications, or reputational damage to the organization if obtained by unauthorized parties or made public (such as strategic planning, financial data, intellectual property, customer and employee data, supply chain, contract terms and pricing, and product quality and safety).
- Existence of protocols and the timeliness of management's response to a cybersecurity incident.

The Guide also notes common sources of cyber threats as:

- Nation-states
- Cybercriminals
- Hacktivists
- Insiders and service providers
- Developers of substandard products and services

© Becker Professional Education Corporation. All rights reserved.

3.2.1 Emerging Risks

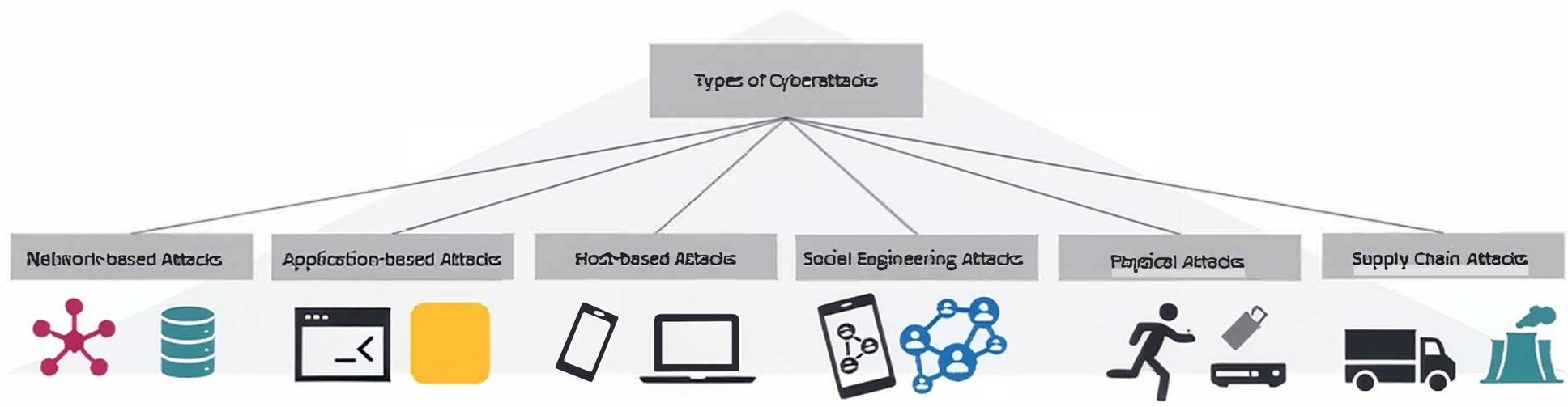
Additionally, there are several factors to consider to help identify emerging risks such as those related to:

- Expansion of technology making it readily available and allowing for an increase in those who have access to an organization's data via the locations in which it is stored (such as the cloud) and through parties such as customers, service providers, and supply chains.
- Increase in the number of devices through which data is accessed and shared by a growing number of global individuals and employees as well as external parties to an organization, such as customers and third-party providers.
- Growth in the number of hackers, hostile parties, and the use of outdated security software, allowing for more sophisticated ways of accessing organizational data and information.
- New and changing regulations and standards relating to the use and access of data, as well as reporting requirements and protocols.

Data analysis tools can also be used to help identify emerging risks and assess internal controls.

3.2.2 Cyberattacks

A cyberattack is any kind of malicious activity that targets computer information systems, infrastructures, computer networks, or personal computer devices and attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. The method of execution of an attack can be grouped into one of the following categories:



- **Network-based Attacks**: These attacks target the infrastructure of a network, including switches, routers, servers, and cabling, with the intent to gain unauthorized access or disrupt operations for users.
- **Application-based Attacks**: These forms of attacks target specific software or applications (desktop or web) such as databases or websites to gain unauthorized access or disrupt functionality.
- **Host-based Attacks**: These attacks target a single host such as a laptop, mobile device, or a server to disrupt functionality or obtain unauthorized access.
- **Social Engineering Attacks**: These attacks involve the use of psychological manipulation or deception to get employees to divulge sensitive information, provide unauthorized access, or assist an attacker in committing fraud. Human interaction through email, text, direct messaging, or social media is the primary medium through which perpetrators gain confidence and trust.

© Becker Professional Education Corporation. All rights reserved.

- **Physical (On-Premises) Attacks**: This is a security breach carried out on an organization's premises or performed in some way that physically involves a bad actor gaining control of sensitive data, hardware, and/or software.
- **Supply Chain Attacks:** These attacks use cyber tactics to target the production and distribution of goods within a supply chain so that there are larger disruptions in the normal operations of a company, government, or other entity.

Illustration 1 Impact of Cyberattacks

Given the interconnections of organizations with their customers, vendors, and partner organizations, the impact of a cyberattack upon one organization could have a profound impact on other organizations. Below are examples of how these attacks could impact stakeholders outside the organization.

Example Attack	Customer Impact	Vendor Impact	Partner Organization's Impact
Ransomware Attack: The attacker encrypted the company's servers and databases, preventing the company from accessing customer data and processing orders	Unable to deliver products to customers, causing interruption of the company's customers' fulfillments	Vendors are unable to communicate with the company through electronic data interchange channels to fulfill purchase orders	Financial losses due to ransom payment to support the victim of the attack
Mobile Code: The attacker infected the company with a virus that deletes critical contact data and spreads the virus through the business network	The customer's ordering systems are infected by the virus, causing data loss	The vendor's systems were infected, causing the vendor to lose critical production data	The partner must reallocate resources to support the company under attack, causing disruptions in its main operations
Malware: The attacker infected the company's servers and exposed confidential customer data	Confidential customer data is exposed to the attacker	Vendor banking information is exposed to the attacker	Reputation loss and potential class-action lawsuit

3.3 Common Cybersecurity Controls

Well-designed cybersecurity controls include policies, procedures, and technology that mitigate threats at all points of discovery and all stages of a counterattack. The controls are usually focused on where the data is being stored, internally or externally.

In situations where the data is stored externally, controls such as service organization control (SOC) reports, right-to-audit clauses, service-level agreements (SLAs), and cybersecurity examination engagements should be considered and included in contracts between the organization and external parties.

Common cybersecurity controls can be grouped into the following categories: preventive controls, detective controls, and corrective controls.

© Becker Professional Education Corporation. All rights reserved.

3.3.1 Preventive Controls

Preventive controls are designed to thwart malicious activity from ever occurring. They attempt to prevent attackers from accessing devices, applications, and networks by employing some of the following tactics:

- **Safeguarding Practices:** Strong preventive software and hardware controls should be coupled with well-designed policies and procedures, such as requiring strong passwords, using multi-factor authentication (MFA), performing background checks, locking devices if unattended, and following strict guidelines regarding sensitive data.
- **Education and Training:** Informing employees about cybersecurity risks and the corporate tools in place to mitigate those risks serves as a preventive control that complements technical safeguards that have been deployed.
- **Regular Security Updates:** Broad and comprehensive security enhancements should occur regularly in order for an organization's physical and logical security measures to be protected against the latest cybersecurity threats.
- **Encryption:** Encrypting data both at rest and in transit involves the process of converting the data into an illegible format based on industry standards so that if the data is comprised or stolen, the hackers will not be able to decipher and use the data for any nefarious purposes.
- **Firewalls:** A firewall monitors and filters traffic based on a set of predefined rules so that only trusted parties and networks can connect or interact with an organization's network, preventing threat actors from compromising the network.
- **Patches:** A patch is an update or modification to an existing software program that is typically released by an application's creator and serves as both a preventive and corrective control that is intended to resolve newly discovered design flaws, operating errors, or gaps that pose cybersecurity risks.

3.3.2 Detective Controls

Detective controls are designed to detect a threat event while it is occurring and provide assistance during investigations and audits after the event has occurred. Examples of detective controls include:

- **Network Intrusion Detection System (NIDS)**: An NIDS is a security solution that monitors incoming traffic on all devices on a network by matching specific elements of that traffic to a library of known attacks and sending system alerts when events meeting predefined criteria are detected.
- **Antivirus Software Monitoring**: Antivirus software works by scanning files in real time and comparing them to a library of known viruses. Scheduled scans of systems should occur automatically and be performed on a regular basis. If viruses are detected, they should be removed, or at least quarantined, immediately. Viruses that can only be quarantined and not removed will require further action by the responsible IT personnel.
- **Network Monitoring Tools**: There are various tools available to monitor a network, such as packet sniffers, which analyze data packets being transmitted on a network; network performance monitoring (NPM) tools that measure network statistics (such as packet loss, system uptime, and availability); or Simple Network Management Protocol (SNMP), which is also used to measure network statistics and error rates.

© Becker Professional Education Corporation. All rights reserved.

- **Log Analysis**: Performing a log analysis involves the recording and monitoring of data to analyze it so that anomalies, trends, or patterns can be detected that may indicate that unauthorized events have occurred. This can be a manual or automated process.
- **Intrusion Detection Systems (IDS)**: An IDS is a security solution that scans the environment to monitor and analyze network or system events for the purpose of finding and providing real-time or near real-time warnings of attempts to access system resources in an unauthorized manner. The key difference between an IDS and an IPS is that an IDS only detects an attack after it has started, but it is unable to prevent it. IDSs can be used by organizations to provide continuous monitoring of the client's network and prevent potential security breaches.

3.3.3 Corrective Controls

Corrective controls are intended to fix known vulnerabilities as a result of recent security incidents, security self-assessments, or changes in industry practices. These controls become preventive or detective once they are put in place and are operating effectively. Examples of corrective controls include:

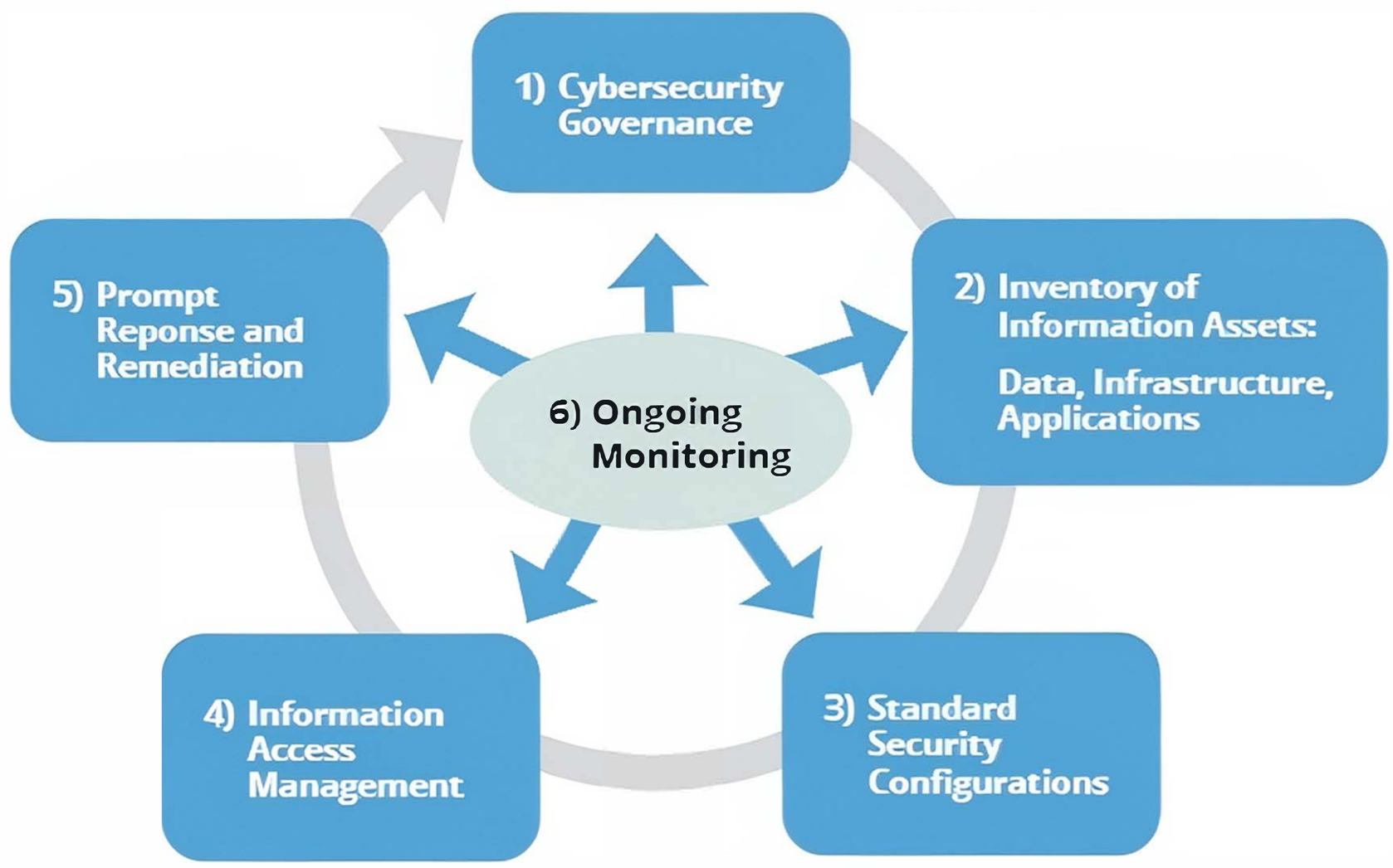
- **Reconfigurations**: Modifying an application or system configuration to rectify known vulnerabilities can restore affected operations and prevent further damage. Examples include revamping firewall rules, retooling an operating system's settings, and altering access control settings.
- **Upgrades and Patches**: Security patches and software or application upgrades may be implemented to accomplish objectives such as enhancing system performance, adding new features, and plugging holes in an organization's security.
- **Revised Policies and Procedures**: Periodically reviewing and revising organizational practices can eliminate some security issues without requiring the purchase of new technology or the modification of existing systems. Revisions may be as simple as splitting one job into two, adding an additional level of review, or changing the way in which sensitive data is handled.
- **Updated Employee Training**: Gaps in employee knowledge about the risk of certain cyberattacks and other forms of IT exploitation can be reduced by training employees to recognize the hallmarks of common fraud schemes, educating them on how to react when suspected fraud occurs, and teaching them how to change existing behavior to prevent future incidents.
- **Recovery and Continuity Plans**: Organizations should have a robust plan in place that allows them to quickly recover from a disaster or attack and continue operating so that the period in which normal business operations are interrupted is minimized.
- **Antivirus Software Removal of Malicious Viruses**: Most modern antivirus programs are designed to not only identify actual or potential viruses but also to expunge those viruses so that they are no longer a threat to the organization.
- **Virus Quarantining**: Isolating actual or suspected viruses removes the threat from the rest of an organization's network and is usually accomplished in an automated manner via antivirus software or manually after suspicious activity has been flagged from the review of system logs.

© Becker Professional Education Corporation. All rights reserved.

3.4 Cybersecurity Risk Assessment Framework

The IIA's *Global Technology Audit Guide: Assessing Cybersecurity Risk, The Three Lines Model*, published in 2020, provides a cybersecurity risk assessment framework with six interdependent components that can be used to assess the design and operating effectiveness of cybersecurity controls and governance. When the components are not designed or operating effectively together, the organization is not well prepared to address cyber threats and emerging risks.

Cybersecurity Risk Assessment Framework



Source: The IIA's *Global Technology Audit Guide: Assessing Cybersecurity Risk, The Three Lines Model* ©2020. The Institute of Internal Auditors, Inc. Licensed for use.

3.5 The Three Lines Model

As noted in The IIA's *Global Technology Audit Guide: Assessing Cybersecurity Risk, The Three Lines Model*, published in 2020, the following three lines play significant roles in addressing cybersecurity risks:

- **The First Line**

  Operational managers serve as the first line roles and are responsible for overseeing and managing data, processes, risks, and controls. Organizations may establish several first line roles for cybersecurity. This may include system administrators and other professionals tasked with protecting the organization's assets.

- **The Second Line**

  The second line roles consist of risk, control, and compliance oversight functions responsible for ensuring that the processes and controls established by the first line are in place and are functioning effectively. These functions often include teams responsible for effective risk management and monitoring risks and threats in the cybersecurity domain.

© Becker Professional Education Corporation. All rights reserved.

The Third Line

As a third line function, the internal audit function provides senior management and the board with independent, objective assurance on governance, risk management, and controls. This includes evaluating the overall effectiveness of the first and second lines in managing and mitigating cybersecurity risks and threats.

Common responsibilities and activities of each line role regarding cybersecurity are summarized as follows:

Roles	Common Responsibilities and Activities for Cybersecurity
The First Line Roles	• Administer security procedures, training, and testing. • Maintain secure device configurations, up-to-date software, and security patches. • Deploy intrusion detection systems and conduct penetration testing. • Securely configure the network to adequately manage and protect network traffic flow. • Inventory information assets, technology devices, and related software. • Deploy data protection and loss prevention programs with related monitoring. • Restrict least-privilege access roles. • Encrypt data where feasible. • Implement vulnerability management with internal and external scans. • Recruit and retain certified IT, IT risk, and information security talent.
The Second Line Roles	• Design cybersecurity policies, training, and testing. • Conduct cyber risk assessments. • Gather cyber threat intelligence. • Classify data and design least-privilege access roles. • Monitor incidents, key risk indicators, and remediation. • Recruit and retain certified IT risk talent. • Assess relationships with third parties, suppliers, and service providers. • Plan/test business continuity and participate in disaster recovery exercises and tests.
The Third Line Roles	• Provide independent ongoing evaluations of preventive and detective measures related to cybersecurity. • Evaluate IT assets of users with privileged access for standard security configurations, problematic websites, malicious software, and data exfiltration. • Track diligence of remediation. • Conduct cyber risk assessments of service organizations, third parties, and suppliers (note: The first and second line roles share this ongoing responsibility).

Source: The IIA's *Global Technology Audit Guide: Assessing Cybersecurity Risk, The Three Lines Model* ©2020. The Institute of Internal Auditors, Inc. Licensed for use.

© Becker Professional Education Corporation. All rights reserved.

4 General and Application IT Controls

4.1 IT Controls: General vs. Application Controls

When identifying and assessing controls during planning, it may be helpful to categorize controls into general and application controls to help understand their purpose and role in mitigating risks.

IT-specific controls can be classified as either IT general controls or application controls (i.e., information-processing controls related to IT applications):

- **IT general controls** are applicable to all system components, processes, and data within an organization or a system environment.
- **Application controls** are controls within an application around input, processing, and output, and are typically applied to individual business processes or application systems.

4.1.1 IT General Controls

IT general controls form the basis of the IT control environment and address the risks arising from the use of IT, which can be categorized as:

- **Applications:** Address risks related to the nature and extent of application functionality and integration.
- **Database:** Address risks arising from the use of IT related to unauthorized updates to the database.
- **Operating System:** Address risks arising from the use of IT related to administrative access, which can facilitate the override of other controls.
- **Network:** Address risks arising from the use of IT related to network segmentation, remote access, and authentication.

Examples of IT general controls that may exist include:

- Controls related to managing access to applications and technology areas
  - **Authentication:** Validate that a user is using their own log-in credentials.
  - **Authorization:** Ensure users only access necessary information (facilitates segregation of duties).
  - **Provisioning and Deprovisioning:** Authorize new and updated user access privileges and the removal of user access.
  - **Privileged Access:** Administrative user access.
  - **User-Access Reviews:** Evaluate user access authorizations over time.
  - **Security Configuration:** System settings of a specific application or IT are to restrict access.
  - **Physical Access:** Physical access to data center and hardware.

© Becker Professional Education Corporation. All rights reserved.

- Controls related to changes to the IT environment
  - **Change-Management Process:** Process to design, program, test, and migrate changes to a production (end-user) environment.
  - **Segregation of Duties Over Change Migration:** Segregate access to make and migrate changes to a production environment.
  - **System Development, Acquisition or Implementation, and Data Conversion:** Process over IT application development or implementation and data conversion.
- Controls related to managing IT operations
  - **Job Scheduling and Monitoring:** Access to schedules and the initiation of jobs or programs related to financial reporting, including oversight of successful execution.
  - **Back-up and Recovery:** Process to ensure financial reporting and operational data are backed up, and such back-up data is available in a timely manner in the event of an outage or attack.
  - **Intrusion Detection:** Monitoring the IT environment for vulnerabilities or intrusion.

4.1.2 Application Controls

Application controls are within an application and are designed to enhance the security and accuracy of data input into the system, strengthening the validity of the outputs from the system.

During the input, processing, and output stages, controls are designed to protect against internal and external threats. The control design that provides this security must be able to adapt in order to continuously provide protection in an ever-changing environment.

- **Input Controls**

  Input controls are designed to ensure that the data entered into the system is both factually accurate and properly authorized. Authorized individuals input data and identifying credentials (a process called credentialing) into the system in order for the input to be accepted. If credentials pass the initial input controls, a second layer of input controls checks that the supplied data meets other established parameters. This second layer includes the technical structure of the data entered, including character types (such as text or numbers) and limit/range checks (such as numerical upper and lower limits), which are just a couple of examples of several different data entry controls.

Illustration 2 Input Controls

An input file containing sales transactions is loaded into the operations system from a retail store at the proper time, carrying the proper credentials for the store and the owner. Input controls accept the authorization for this file to be read into the system. However, during the initial read, the file is seen to be less than half the size of a typical file for that store during this time of year. Because the number of sales transactions is too low (outside of the lower limit for this input control), a contingency trigger interrupts processing and sends notifications to both the store manager and the operations analyst to check to make sure the entire file was transmitted. Processing resumes when an authorized person (the store owner or operations analyst) submits their credentials and replaces or confirms the input file.

© Becker Professional Education Corporation. All rights reserved.

Processing Controls

Processing controls are designed to ensure that transformations to the input data are executed correctly and that all data communication during processing is appropriately secured.

- The most basic type of processing control is an audit trail, which involves the creation of a record during particular steps within a process in order for a control to be reviewed by other employees or potential auditors. By examining this processing control, error or fraud may be discovered and traced to the specific processing step where it occurred.
- Another processing control is security over system processing. Files that have been created by an audit trail and any other data that has been processed must be secured for use only by authorized persons and authorized systems for further processing. Security processing controls involve credentialing for report files as well as the use of secure file transfer protocols (to transfer files from one process or location to another) and file encryption.
- Information processing controls can be automated or manual and applied to the processing of information and transactions, and can help to ensure that transactions occur, are authorized, and are completely and accurately processed and reported. Such controls help to ensure the integrity of the data in an entity's information system.

Illustration 3 Processing Controls

An analyst receives transaction reports from each retail store in the corporation and uses a program to consolidate the files into one report containing all transaction records in chronological order for the day. Each day, the analyst preserves the individual store reports and the consolidated reports in the company's cloud-based file storage system.

Another analyst later takes the consolidated file and uses it as input to another program in order to organize the sales by store owner (some owners have multiple retail stores) to calculate royalties owed to the parent company. The second analyst also saves the consolidated file (the output from the first process that is now the input for the second process) and the new output file detailing sales by owner in the company's file storage system, where it can be used by other analysts for different purposes.

The benefits of following this process control include error detection, fraud detection, and promotion of good business continuity practices. The first analyst's output file should be identical to the second analyst's input file. Any other analyst should be able to run the same program against the same input file stored on record and get the same output file stored on record. If the files are not the same or the output results are different, then it is possible that an error or fraud has occurred, or that the data became corrupted. Lastly, with backups in existence, if a data file was corrupted, lost, or stolen, then work can proceed from the most recent backup.

© Becker Professional Education Corporation. All rights reserved.

- **Output Controls**

  Output controls are designed to ensure that the results of system processing are presented in a useful state to only authorized persons and processes. Credentialing, secure file transmission, and file encryption are output controls used to protect output from misuse or theft. Output controls should also be triggered when a process makes a recommendation that is highly risky or unusual. In such cases, analysts and executives should review the recommendation before authorizing it. For example, if a computer process produces an output that reflects an unusually high order quantity in a period when sales are sharply decreasing, output controls should require managerial approval instead of automatically approving the high order quantity.

Illustration 4 Output Controls

Interest rates on loans are calculated from economic factors such as national savings rates, the consumer price index, currency exchange rates, and stock and bond market activities. These calculations may occasionally result in a recommended interest rate being negative, meaning that the bank should pay the borrower interest to take out a loan. It is sometimes appropriate for a bank to use negative interest rates, but less often than such calculations may recommend. A prudent output control would require an executive-level bank manager to approve or modify any system recommendation for a negative interest rate.

- **Storage Controls**

  Storage controls are designed to ensure that the appropriate records are retained, retrieved, and accessed only by authorized people and processes. Stored data must be protected in several ways:

  - **Physical controls** help to secure the physical location of the data. Examples of physical controls are controlled access, air gaps (computers physically isolated from the internet or other systems), and security patrols.
  - The use of **processing and storage sites** hosted by a third-party provider should require the use of legal contracts to limit access to a customer's stored data by the hosting organization. Detection controls are designed for the stored data to ensure contract compliance.
  - A **version control system** provides an additional layer of security and provides the additional benefits of keeping system files in date order and creating automatic backup copies of the files or information systems. In the event a file or system needs to be reloaded from a backup, the backup can be accurately selected from a source dated prior to the observed problem.

4.2 The IT Control Hierarchy

An alternative way to categorize IT controls follows a top-down hierarchy of IT governance controls, IT management controls, and IT technical controls. Such classification of IT controls can be linked to the classification of IT general versus application controls.

© Becker Professional Education Corporation. All rights reserved.

At the bottom of the hierarchy are the IT technical controls that include application-based controls. The remaining two categories of IT management controls and IT governance controls are comprised of IT general controls that include:

- systems development controls;
- systems software controls;
- physical and environmental controls;
- organization and management;
- standards; and
- policies.

The different layers may overlap between the categories and interconnect with each other.

Pass Key

IT controls can be classified as IT general controls and application controls:

- **IT general controls** are applicable to all system components, processes, and data within an organization or system environment.
- **Application controls** are controls within an application around input, processing, and output and are typically applied to individual business processes or application systems.

Pass Key

IT controls can also be categorized in a hierarchy of IT governance controls, IT management controls, and IT technical controls:

- **IT governance controls** include policies applying to all IT governances.
- **IT management controls** include three components:
  1. Standards
  2. Organization and Management
  3. Physical and Environmental Controls
- **IT technical controls** also include three components:
  1. System Software Controls
  2. Systems Development Controls
  3. Application-based Controls

These classifications are interrelated in the sense that the "Application-based Controls" component of the IT control hierarchy is considered an application control, whereas the other components fall into the category of IT general controls.

© Becker Professional Education Corporation. All rights reserved.

5 IT Control Frameworks

The main purpose and benefit of adopting an IT control framework, such as COBIT, COSO, NIST, or ISO control framework, is to provide a structured way of designing controls to ensure that IT-related risks in an IT environment are sufficiently and adequately addressed. An IT control framework is a useful tool in performing a comprehensive IT risk assessment.

While a formal framework will facilitate the organization's compliance with the various regulatory or statutory requirements, an informal framework can also be acceptable depending on the organization's needs.

The selection or development of the IT control framework should involve all relevant stakeholders, including the business process owners and the individuals responsible for implementing the controls. The framework should apply to the entire organization and be used by the internal audit function in planning and performing work.

When planning and performing IT control reviews, the CAE or designated supervisors need to ensure that all factors are considered. A checklist can be used by internal auditors to examine the organization's IT control framework and ensure that all control elements are addressed.

Pass Key

The main purpose and benefit of adopting an IT control framework is to provide a structured way of designing controls to ensure that IT-related risks in an IT environment are sufficiently and adequately addressed.

It is a useful tool when performing a comprehensive IT risk assessment.

6 Data Privacy

6.1 Data Privacy

Data privacy is a significant issue, covered by various laws and regulations, and can create risks for an organization that may need to be addressed as part of the engagements performed by the internal audit function. Therefore, data privacy should be considered when assessing key risks and controls during engagement planning.

Data privacy is the right of individuals to control their personally identifiable information (PII), including how the information is collected, handled, used, and accessed. Privacy is crucial for corporate data. Clear communication of organizational privacy policies, ongoing monitoring, and deployment of adequate controls help safeguard corporate data from privacy concerns.

© Becker Professional Education Corporation. All rights reserved.

6.2 Data Privacy Principles

The common data privacy (protection) principles recognized by The Institute of Internal Auditors (The IIA) are aligned with those in the General Data Protection Regulation (GDPR):

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

6.2.1 Data Privacy Laws and Regulations

Privacy laws exist to protect an individual's private life and keep personal details out of the public domain. These laws also create trust between consumers and enterprises so that when a consumer's personal information is shared, such as with a credit card company or a healthcare provider, sensitive information will be safeguarded according to rules outlined in applicable privacy regulations.

Privacy laws regulate how those entrusted with private information must collect, process, maintain, and disclose it. Generally, those entrusted with the information must be clear about what data they collect, keep it confidential, and limit access to only those who need it.

Today's modern privacy laws in the United States focus on particular types of data or entities, such as healthcare data (e.g., the Health Insurance Portability and Accountability Act [HIPAA]), financial data, or data held by federal agencies. There is no single federal law that applies generally and regulates all personal data.

Unlike the United States, the European Union enacted one comprehensive data privacy law, the General Data Protection Regulation (GDPR), that applies generally and governs how all entrusted with personal data should handle such information.

6.2.2 General Data Protection Regulation (GDPR)

Effective May 2018, GDPR became the European Union's general applicability law regulating the privacy of data. GDPR provides circumstances when it is lawful to process personal data, such as with proper consent or when complying with a legal obligation. This law is one of the strictest privacy laws in the world, as it imposes steep penalties for violators, with fines reaching millions of dollars. Although enacted by the EU, the law's scope extends beyond the EU. GDPR applies to any of the following:

- Data processors based in the EU, even if the actual processing takes place outside of the EU.
- Data processors not based in the EU if the processor is offering goods or services to those in the EU or is monitoring the behavior of those in the EU.
- Data processors not based in the EU but where EU law applies via public international law (e.g., EU embassies).

© Becker Professional Education Corporation. All rights reserved.

GDPR provides principles that must be followed when processing data:

- **Lawfulness, Fairness, Transparency**: Data must be processed lawfully, fairly, and in a transparent manner.
- **Purpose Limitation**: Data must be processed for specified, explicit, and legitimate purposes. Further processing beyond the purpose is permitted for public interest archiving, scientific or historical research, or statistical purposes.
- **Data Minimization**: Data processing must be adequate, relevant, and limited to what is necessary for the purpose.
- **Accuracy**: Data must be accurate and kept updated.
- **Storage Limitation**: Data must be stored only for as long as is necessary. Storing it for longer periods is permitted for public interest archiving, scientific or historical research, or statistical purposes.
- **Integrity and Confidentiality**: Data must be processed securely and protected against unauthorized or unlawful processing, accidental loss, destruction, or damage.
- **Accountability**: Evidence of the compliance with data privacy regulations.

Pass Key

The data privacy principles from the GDPR are:

- Lawfulness, Fairness, Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

6.3 Data Privacy Controls

Data privacy controls are essential for mitigating the risks associated with the potential misuse, leaks, or loss of personally identifiable information (PII). Implementing strong data privacy measures not only protects the PII of customers, employees, donors, and business partners but also safeguards an organization's public image and brand reputation.

By prioritizing data privacy, organizations build credibility and foster trust, generating goodwill that can lead to a significant competitive advantage. Furthermore, robust data privacy controls ensure compliance with relevant regulations and legal frameworks, avoiding potential penalties and reputational damage.

© Becker Professional Education Corporation. All rights reserved.

Examples of general controls for data privacy include:

- Adequate governance and oversight by the board and senior management.
- Benchmarking the organization's privacy compliance and data-handling practices against international policies, laws, regulations, and best practices.

Characteristics of an effective data privacy program may include:

- Clearly defined roles and responsibilities.
- An established privacy statement as well as policies and procedures for collecting, using, disclosing, retaining, and disposing of PII.
- Established practices and plans for data privacy protection, incident response, and corrective actions.
- Regular assessments of privacy risks and the maturity of privacy models.
- Adequate training and education of employees on data privacy.
- Controls over external service providers to safeguard data privacy.

6.4 The Organization's Data Privacy Framework

When assessing the organization's data privacy framework, internal auditors should determine:

- whether there exists a data privacy framework;
- whether the board has set a risk appetite for privacy risks;
- whether the framework is effective in identifying and addressing significant privacy risks;
- how the data is classified according to the privacy framework and relevant policies as well as the appropriateness of the classification and related controls; and
- whether there exist privacy incident response plans.

Additionally, internal auditors should gain an understanding of the context of internally used and externally communicated (e.g., to customers) data privacy and security policies. They may seek collaboration with other parties, such as legal counsel, data privacy professionals, and IT specialists, as follows:

- Working with legal counsel to identify additional steps to evaluate the privacy framework
- Consulting privacy professionals to understand the maturity of the privacy framework
- Collaborating with IT specialists to create a process map of information flows, system controls, and the PII life cycle, including incident response programs

6.4.1 Assessing Privacy Risks

Internal auditors may focus their assessment on the following privacy risks when evaluating the data privacy framework:

- **Legal and Organizational Risk**

  Internal auditors play a crucial role in ensuring data privacy by verifying that responsible parties are aware of relevant laws and regulations and that employees understand the expectations and consequences of noncompliance. They assess staff competency and their approaches to staying updated on evolving legal requirements and technological advancements. Proof of compliance through proper documentation should be preserved. Furthermore, internal auditors analyze whether expenditures on privacy controls are cost effective. For instance, excessive spending on encryption for routine data may be viewed as an unnecessary cost.

© Becker Professional Education Corporation. All rights reserved.

- **Infrastructure Risk**

  The processing of PII involves various formats and platforms—from paper forms to online systems, data entry points, and automated processes. Each step of the process may introduce potential vulnerabilities to privacy. Internal auditors should track PII in both its operations and in backup storage. This involves evaluating encryption protocols for both stored and transmitted data.

  Effective PII controls include:

  - Physical safeguards such as shredders and locked files.
  - Robust IT general and application controls.

  A comprehensive data map and inventory of all PII should be established across all platforms, including third-party transfers.

- **Application Risk**

  When evaluating software applications, internal auditors should focus on reviewing privacy risk assessments and whether "privacy by design" principles are implemented. This includes verifying that there is proper data classification, defaults to the least privilege for user access, and secure external interfaces with proper authorization limits.

- **Business Process Risk**

  While PII is essential for business operations, its use introduces risks, particularly when handled in physical formats like printed documents. Internal auditors should verify that organizations implement basic controls to mitigate these risks, especially in areas open to the public. Such controls include promoting clean desks and ensuring computers are locked when not in use.

7 Data Security

7.1 Data Security Policies and Practices

Data security policies and practices are typically used to assist with risk assessment, compliance with standards, laws, and regulations, and in the ongoing monitoring of risks and controls. They include aspects such as physical security measures, controls, backup and recovery procedures, incident response protocols, and employee training.

Considering data security policies and practices during engagement planning helps to identify key risks and controls. The focus of such policies and practices is on protecting the confidentiality, integrity, and availability of information that aligns with some of the data privacy principles.

© Becker Professional Education Corporation. All rights reserved.

With the development of new technologies and the trend of outsourcing, it is challenging to keep track of where data is stored, how it is protected, who has access to it, and whether it is disposed of securely. The CAE or designated supervisors can consider the following to understand the sufficiency of the organization's data security practices, which may help to identify risks and controls:

- Whether there exists a board committee overseeing the determination of risk appetite over privacy risk.
- Understand the management's risk appetite over privacy risk.
- Recognize applicable privacy laws and regulations.
- Whether there are established privacy procedures and programs within the organization, with defined responsibilities and accountabilities and sufficient resources to ensure its efficiency.
- Gain knowledge of the PII being collected and whether any PII is disclosed to or processed by third parties.
- Who defines what is considered private, and the consistency and appropriateness of the definitions.
- How PII is protected in the database, network, system platform, application, and business process layers.
- Whether data privacy-related training is provided to relevant employees.
- Whether the effectiveness of privacy programs is assessed on a regular basis by management to determine the need for updates in order to meet new requirements.

Pass Key

The "CIA Triad" is a common concept used to describe key elements that data security policies and practices focus on:

Confidentiality: Authorized access and handling of data and information

Integrity: Accuracy of the data and information

Availability: Access to the data and information when needed

© Becker Professional Education Corporation. All rights reserved.

NOTES

© Becker Professional Education Corporation. All rights reserved.

MODULE

4 Business Continuity and Disaster Recovery

Part 2
Unit 1

This module covers the following topics from the *CIA examination syllabus*:

CIA Syllabus—Section A: Engagement Planning
3. Plan the engagement to assess key risks and controls *May include but is not limited to:* d. When planning an engagement, recognize business continuity and disaster recovery readiness concepts such as business resilience, incident management, business impact analysis, and backup and recovery testing

1 Business Continuity and Disaster Recovery

The internal audit function may perform engagements relating to business continuity management (BCM) and crisis management (CM), which is a key component of BCM. Such engagements are described by The IIA's *Global Practice Guide: Business Continuity Management*, published in 2014:

- Assurance engagements may be performed to verify that BCM and CM are effective. The scope of assurance engagements may include a comprehensive BCM program or specific elements (e.g., testing the occurrence and update frequency of the business continuity plan [BCP], and the maturity of the crisis management plan [CMP]). The internal audit team's knowledge of the risks mitigated by the BCP or CMP and prior involvement in an advisory capacity during plan development may promote a more efficient engagement planning process.
- Advisory services may be performed to help management focus planning activities and coordinate BCM and CM with risks and controls.

Therefore, during engagement planning for such engagements, internal auditors may consider key risks and controls related to business continuity and disaster recovery readiness. Key concepts such as business resilience, incident management, business impact analysis, and backup and recovery testing help organizations prepare for, respond to, and recover from unexpected events, minimizing downtime and safeguarding critical operations.

When identifying risks and controls, the existence, sufficiency, and appropriateness of the following factors can be considered:

- Storage—location of where data, systems, and applications are stored and threats to those locations
- Recovery—backups and protocols to enable data, systems, and applications to be restored if compromised
- Resources—appropriate human resources to help with identifying, implementing, and executing policies and practices to identify, address, and mitigate risks

© Becker Professional Education Corporation. All rights reserved.

1.1 Business Resiliency

Business resiliency is the integration of system availability controls, disaster recovery plans, business continuity plans, and crisis management plans into a central set of procedures to consider whether an organization can continue to operate or quickly return to operations without irreparable harm to its people, information, or assets.

Organizations must identify what activities are necessary to the core operations of their organization and assess existing threats to those activities. Once critical systems and processes are identified, management can begin building a business resiliency program to determine whether these vital functions can quickly be repaired and put back into operation given a business crisis or disruption.

Pass Key

- **Business resiliency** is the overall integration of procedures implemented to keep operations running smoothly
- Disaster recovery, business continuity, and crisis management plans are different potential components of a business resiliency program.
  - — **Disaster recovery** focuses on IT functions
  - — **Business continuity** focuses on non-IT, operational, and personnel functions
  - — **Crisis management** focuses on large-scale incidents that are considered a crisis

1.2 Crisis and Incident Management

1.2.1 Crisis Management

In terms of business operations, a crisis is an unexpected, large-scale incident that can cause major negative effects on an organization and its stakeholders. The circumstances that define a crisis vary between organizations. Organizations conduct risk analyses to identify events that would result in significant adverse impacts and constitute disasters.

Crisis management policies are vital, as a crisis presents stressful situations that involve important decisions that must be made quickly. These decisions can be difficult if an organization does not have clearly defined roles, responsibilities, and procedures.

The goals of a crisis management plan should be to lessen the impact of the crisis, protect people, protect organizational reputation, and return to normal operations as soon as possible.

In the event of a crisis, data may need to be recovered from a variety of IT systems and information management systems. This may include data centers, servers, networks, remote access services, document management systems, and data from applications, such as:

- Critical systems: Related to organizational core processes, and often includes telecommunications, payroll, and order processing
- Vital systems: Finance and customer service systems
- Sensitive systems: Contain confidential or personal data, such as payroll systems
- Noncritical systems: Human resources, budgeting, and purchasing

© Becker Professional Education Corporation. All rights reserved.

The risks related to business continuity management identified during engagement planning would be assessed by the likelihood and magnitude of impact and the restoration priorities considered.

Crisis management policies should address the following:

- Risk assessment of what potential crises the organization could face and how to properly respond
- Procedures for implementation, including the steps management and employees must perform to put the plan into operation
- A crisis response command center, where directives originate during a crisis (a physical or virtual location)
- Defined crisis management roles and responsibilities for those who oversee all final decisions and the roles and responsibilities of each individual
- Established internal and external lines of communication, so parties can communicate during a crisis
- Employee training on crisis management policies and procedures, so that employees understand all necessary courses of action during a crisis

1.2.2 Incident Management

Incident management is similar to crisis management, except on a smaller scale. Crisis management has a broader impact on the organization, whereas incident management addresses a smaller situation that can be more easily managed. As defined by The Institute of Internal Auditors (The IIA) in the *Global Practice Guide: Business Continuity Management*, published in 2014:

- **Crisis:** An event that, if not handled appropriately, may significantly impact an organization's ability to operate, remain profitable, and manage reputational risk. Commonly, these are natural or physical disasters, failures of critical operations and/or connectivity, disruptions to key business partner relationships, and technology exposures.
- **Incident:** An event that is not part of operational standards, which may temporarily impact an organization and, in some cases, could lead to an emergency or disaster.

Pass Key

Crisis management relates to the response to an unexpected, large-scale incident that can cause major negative effects on an organization and its stakeholders.

Incident management addresses a smaller situation that can be more easily managed and that does not have as large an impact as a crisis. However, in some cases, an incident may lead to a disaster or emergency.

1.3 Business Impact Analysis (BIA)

Identifying and assessing risks is a key component in building a business resiliency program. This assessment can be done by performing a business impact analysis (BIA). This analysis identifies the business units, departments, and processes that are essential to the survival of an organization as well as the organizational impact in the event of failure or disruption.

© Becker Professional Education Corporation. All rights reserved.

The BIA will identify how quickly essential business units and/or processes can return to full operation following a disaster. The BIA will also identify the resources required to resume business operations. For example, a specific department may utilize custom hardware/software, operate in locations with challenging geographic or weather conditions, or depend on third-party vendors.

- Under a **high-impact (H)** category, the department:
  - cannot operate without this resource;
  - may experience a high recovery cost; or
  - may fail to meet the organization's objectives or maintain its reputation.
- Under a **moderate- or medium-impact (M)** category, the department:
  - could partially function temporarily for a period of days or a week;
  - may experience some cost of recovery; or
  - may fail to meet the organization's objectives or maintain its reputation.
- Under a **low-impact (L)** category, the department:
  - could operate for an extended period of time; or
  - may notice an effect on achieving the organization's objectives or maintaining its reputation.

The BIA is made up of the following steps:

1. **Establish the BIA Approach**: Agreement on the necessary approach to performing the BIA is critical and must first be clearly outlined by the organization. During this phase, executives and relevant managers define the impact types and criteria, as well as the time frames to observe and the methodology to use.
2. **Identify Critical Resources**: Management must clearly define critical functions in the organization and delineate which IT resources are required to perform them. This will highlight organizational processes that are the most vulnerable to disruption. This step involves a combination of interviews with key personnel and documentation review.
3. **Define Disruption Impacts**: In this phase, the organization must identify and evaluate the impact of a service disruption by understanding its effects over time and the resources negatively affected or required to deal with the disruption. Risks can include quantitative or qualitative effects and may be natural or human-inflicted threats.
4. **Estimate Losses**: This step involves the management team outlining an exhaustive list of potential risks and events that could occur that would disrupt operations and assigning each of those threats a probability of likelihood. This probability is referred to as the annualized rate of occurrence (ARO). Potential losses can be quantified by using the ARO and variables to calculate the annualized loss expectancy.
5. **Establish Recovery Priorities**: Management must prioritize recovery strategies to decide which tasks personnel should address first. This will vary depending on the maximum outage time that a particular resource can handle, with those resources that have a lower tolerance threshold targeted first. For example, resources that can only be down four hours before a significant impact to the organization occurs will be addressed before a resource that can be down 24 hours.

© Becker Professional Education Corporation. All rights reserved.

6. **Create the BIA Report**: These reports may be completed at the department level, business unit level, product level, or by any other appropriate means of segregating an organization to evaluate risk, as long as all known risks have been addressed. These individual reports can then be combined to form an organization-wide BIA.
7. **Implement BIA Recommendations**: This phase involves senior management evaluating the comprehensive BIA report, determining which risks pose the greatest threat, and implementing preventive or corrective actions to remediate those threats.

Pass Key

The steps in business impact analysis (BIA) may be summarized as:

- Identify business processes and resources.
- Estimate the impacts and losses.
- Determine recovery times and priorities.

1.4 Business Continuity Plans (BCPs)

Disaster recovery plans are focused on restoring the IT infrastructure during a disaster, while business continuity plans are focused on keeping the business operational. Business continuity plans are more comprehensive than disaster recovery plans and contain contingency and mitigation procedures around all business processes, including relocating facilities, human resource tasks, and managing relationships with customers and suppliers.

The overall goal of the business continuity plan will be how to continue operations or restore operations in the most efficient and effective manner possible with consideration given to all aspects of the organization.

Business continuity plans must consider the following:

- Identify the organization's key business processes.
- Identify the risks that exist in key business processes.
- Determine the acceptable downtime for key business processes.
- Implement mitigation and contingency plans to address risks and downtimes.

Additionally, a business continuity plan can include:

- Stakeholder communication plan
- Data backup procedures
- Disaster recovery plans (restoration of information systems after a disaster)
- Business impact analysis (BIA)
- Incident response procedures

© Becker Professional Education Corporation. All rights reserved.

Illustration 1 Business Continuity Plan

A health insurance organization serving members nationwide reviews its business continuity plan annually. The organization's main office is located in a region where hurricanes threaten business operations each year. Although most of the organization's employees work remotely, many lose internet access during natural disasters, making them unable to work from their homes.

As part of its business continuity plan, the organization relocates a core team of employees to a safe, operational facility. The facility is secure and has internet access and telephone services. Additionally, the organization moved all critical applications and systems to the cloud several years ago as part of its business continuity plan. By using the cloud, the organization can determine whether, in the event of a disaster, the relocated core team can resume necessary business operations on behalf of the organization.

1.4.1 IT Contingency Planning

A business continuity management plan should include IT (or information system) contingency planning. The goal of IT contingency planning is to mitigate business risks due to an IT disruption caused by hardware or software, a vendor, a supplier, devices, or an external interface or environment.

An IT (or information system) contingency plan is a strategy used to help recover information systems, operations, and data after a processing disruption that can include:

- Using alternate equipment to restore information systems.
- Locating another physical location to use to recover information systems operations.
- Using other (manual) methods such as email or phone to reestablish communication and perform the affected processes (in the short-term).

IT contingency planning consists of forming and testing a plan, incident handling (i.e., crisis management), and disaster recovery.

1.5 Disaster Recovery

1.5.1 Overview

A major component of a business resiliency program is disaster recovery. Disaster recovery consists of an organization's plans for restoring and continuing its information technology function in the event of the destruction of not only program and data files, but also computer processing capability.

Short-term problems or outages do not normally constitute disasters. If processing cannot be quickly reestablished at the original processing site (possibly because the original processing site no longer exists), then disaster recovery is necessary.

© Becker Professional Education Corporation. All rights reserved.

Disaster recovery and business continuity plans are part of overall risk management. If disaster strikes or business is interrupted and plans are not already in place, the organization may go out of business.

- The advantage of having plans in place is being able to continue operations with minimal disruptions (i.e., operations and cash flow continue).
- The disadvantage of having plans in place is the cost and effort required to establish and maintain these plans.

1.5.2 Steps in Disaster Recovery

The steps in a disaster recovery plan are to:

1. assess the risks;
2. identify mission-critical applications and data;
3. develop a plan for handling the mission-critical applications;
4. determine the responsibilities of the personnel involved in disaster recovery; and
5. test the disaster recovery plan.

An organization's disaster recovery team consists of key operations management personnel and, for larger entities, a disaster recovery services provider. If application software packages are utilized, the package vendors may be involved. For distributed processing, hardware vendors may be involved. Senior management support is absolutely necessary for an effective disaster recovery plan.

1.5.3 Backup and Recovery Approaches

- **Use of a Disaster Recovery Service**

  Disaster recovery service providers, referred to as disaster recovery as a service (DRaas) or managed service providers (MSPs), may provide a simple backup of data or more complex services, such as systems file syncing, to ensure data loss prevention and coordinate recovery plans among different systems, applications, infrastructure, and even full IT environment replication.

- **Internal Disaster Recovery**

  Organizations with the requirement for instantaneous resumption of processing after a disaster (e.g., banks and houses) may provide their own duplicate facilities in separate locations. Data might be mirrored (i.e., updated and stored in both locations), and processing can be switched almost instantaneously from one location to another. A duplicate data center and data mirroring are expensive, and most organizations adopt cheaper solutions.

- **Multiple Data Center Backups**

  Organizations can use one data center to back up another or back up to a cloud provider, assuming that there is enough capacity to process the essential applications. Organizations also must decide what types of backups to perform in order to recover lost data.

  - Full backup is an exact copy of the entire database. Full backups are time consuming, so most organizations only do full backups weekly and supplement them with daily partial backups.

© Becker Professional Education Corporation. All rights reserved.

- Two types of partial backups are possible:
  - An incremental backup involves copying only the data items that have changed since the last backup. This produces a set of incremental backup files, each containing the results of one day's transactions. Restoration involves first loading the last full backup and then installing each subsequent incremental backup in the proper sequence.
  - A differential backup copies all changes made since the last full backup. Thus, each new differential backup file contains the cumulative effects of all activity since the last full backup. Consequently, except for the first day following a full backup, daily differential backups take longer than incremental backups. Restoration is simpler, however, because the last full backup needs to be supplemented with only the most recent differential backup instead of a set of daily incremental backup files. Many organizations make incremental and differential backups daily.

- **Alternative Processing Facilities**

  Organizations can have off-site facilities for storage of data, operating systems, documentation, etc., such as:

  - **Cold Site:** A cold site is an off-site location that has all the electrical connections and other physical requirements for data processing, but it does not have the actual equipment. Cold sites usually require one to three days to be made operational because equipment has to be acquired. Organizations that utilize a cold-site approach normally use generic hardware that can be readily (and quickly) obtained from hardware vendors. Cold sites are the cheapest form of off-site location.
  - **Warm Site:** A warm backup site falls somewhere between a cold site and a hot site. It is a facility that already has hardware installed but will fall short of the processing capabilities typically found in a hot site or at the actual business during normal operations due to a lack of fully operational computer and office equipment. The warm backup site is the compromise between the hot backup site and the cold backup site.
  - **Hot Site:** A hot site is an off-site location that is equipped to take over the organization's data processing as these locations are not only pre-wired for use but also include the necessary hardware and office equipment to perform the functions of the organization. Backup copies of essential data files and programs may also be maintained at the location or a nearby data storage facility. Hot sites are more expensive than cold or warm sites.

  The following matrix depicts key characteristics of each of these sites:

	Location	Connections in Place?	Equipment in Place?	Days to Be Operational	Cost
Cold Site	Off-site	Yes	No	1–3 days	Cheapest
Warm Site	Off-site	Yes/No	Yes/No	0–3 days	Moderately expensive
Hot Site	Off-site	Yes	Yes	Immediately	Most expensive

© Becker Professional Education Corporation. All rights reserved.

Other options may include:

- Reciprocal agreements made with other organizations to share resources in the event of a crisis
- A time-share agreement in which two organizations co-lease a backup facility

Under these agreements, it is important for management to ensure software and hardware compatibility between the organizations. Without compatibility, it can be difficult or, in some cases, impossible to restore data.

1.5.4 Backup and Recovery Processes

Backing up all program and data files regularly is necessary both for recovery in a disaster scenario and for recovery from processing problems. Copies of key master files and records should be stored in a secure remote site located outside of the organization. Copies of files kept on-site should be stored in fireproof containers or rooms.

- **Backup of Systems That Can Be Shut Down:** The backup process is relatively simple when a system can be shut down for backup and maintenance. When this is the case, files or databases that have changed since the last backup (or just all data) can be backed up, using the son-father-grandfather or similar concept.
- **Backups of Systems That Do Not Shut Down:** Effective backups are more difficult when an information system cannot be shut down. Recovery often includes applying a transaction log (a file of the transactions that had been applied to the databases) and reapplying those transactions to get back to the point immediately before the failure.
- **Mirroring:** Mirroring is the use of a backup computer to duplicate all of the processes and transactions on the primary computer. Mirroring, which can be expensive, is sometimes used by banks and other organizations for which downtime is unacceptable.
- **Split-Mirror Backup:** As the amount of data needed to support many large organizations grows, so do the time and resources that it takes those organizations to back up and recover their data. One often-used, effective backup method is known as a split-mirror backup, which is useful when the main systems must always be online. A split-mirror backup uses a remote server to back up large amounts of data offline that can be restored in the event of a disaster. A split-mirror backup may be used either by the organization internally or in conjunction with a disaster recovery service provider.

1.6 Backup and Recovery Testing

An effective control is backup and recovery testing. Testing is the most effective method to ensure that a business continuity or disaster recovery plan stays current and functional.

- Tests should be conducted periodically. Most mature organizations test their plans once or twice per year, but the testing frequency may increase due to the following factors:
  - Changes in business processes
  - Changes in technology
  - Changes in team members responsible for overseeing and executing the plan
  - Expected events that could potentially disrupt business operations (e.g., an anticipated hurricane season)
- Tests should cover a range of threats, scenarios, and various components within the plan.
- A structured process must be in place to identify issues and gaps revealed during testing and to monitor their resolution effectively.

© Becker Professional Education Corporation. All rights reserved.

NOTES

© Becker Professional Education Corporation. All rights reserved.

MODULE

5 Finance and Accounting Concepts

Part 2
Unit 1

This module covers the following topics from the *CIA examination syllabus*:

CIA Syllabus—Section A: Engagement Planning
3. Plan the engagement to assess key risks and controls *May include but is not limited to:* e. When planning an engagement, recognize finance and accounting concepts related to the activity under review such as current and fixed assets, short-term and long-term liabilities, capital, and investments

1 Corporate Finance Concepts

1.1 Overview of Finance Concepts

The internal audit function may be asked to perform engagements relating to finance processes and activities, including those relating to investment decisions, financing decisions, and dividend decisions. Therefore, it is important to understand finance concepts to be able to identify risks and controls during planning for such engagements. When considering risks, some assertions to consider include authorization and approval, accuracy, valuation, and compliance.

Finance can be described as a management decision-making role that deals with:

- Performing financial planning and analysis.
- Allocating funds for investments and expenses.
- Securing and sustaining funding sources.
- Fulfilling current financial obligations.
- Ensuring the organization maintains adequate liquidity or cash flow to meet obligations on time.

The goal of corporate finance is to maximize the economic value of the organization over the long term. The finance function within an organization plays a significant role in monitoring the organization's performance. This can be accomplished, for example, by analyzing the variance between expected outcomes and actual results, as well as by calculating and evaluating financial ratios. Insights gained through these analyses have a significant impact on key decisions in corporate finance.

© Becker Professional Education Corporation. All rights reserved.

Another key aspect of corporate finance is financial risk analysis, which involves identifying, assessing, and managing various risks the organization may face. These risks may include:

- Risks associated with capital budgeting decisions.
- Counterparty risks, or the potential inability of others to meet their financial or contractual obligations to the organization.
- Risks related to foreign exchange fluctuations, interest rates, and other factors in international trade.
- Risks arising from the use of complex financial instruments.

1.2 Investment Decisions

Investment decisions include short-term decisions to meet the need for capital preservation, liquidity (ability to convert an asset into cash quickly) maintenance, and/or the achievement of a reasonable return on investment.

Investment decisions also include long-term decisions, the primary objective of which is to invest in assets yielding returns that exceed the cost of capital. The decision process involves capital budgeting and financial analysis to support long-term investment projects.

1.2.1 Capital Budgeting

Capital budgeting is a process for evaluating and selecting the long-term investment projects of the organization. Proper capital budgeting is crucial to the success of an organization. The amount of cash the organization takes in and pays out for an investment affects the amount of cash the organization has available for operations and for other activities of the organization. One of the primary goals of capital budgeting is to implement capital projects that increase the value of the organization to the shareholders (maximize shareholder wealth).

Developing and implementing a capital budget for a project involves five major stages, as follows:

1. Identify and define potential investment opportunities.
2. Estimate the cash inflows and outflows and risk for each potential investment.
3. Analyze the profitability of each potential investment using discounted cash flow methods and select the investments that maximize profitability.
4. Implement the selected investments.
5. Monitor the investments and conduct a post-audit to evaluate the effectiveness and efficiency of each investment.

The following principles are used in capital budgeting:

- Decision making is based on cash flows, not accounting profits.
- The timing of cash flows is important.
- Cash flows include incremental costs and opportunity costs but exclude sunk costs.
- Cash flows are considered on an after-tax basis.
- Financing costs are considered in the hurdle rate and are not considered a cash outflow.

© Becker Professional Education Corporation. All rights reserved.

1.2.2 Investment Analysis Methods

The simple rate of return, also known as the accounting rate of return (ARR), evaluates a project's profitability based on its net operating income rather than its cash flow. This method involves estimating the revenue a proposed investment will generate and subtracting all anticipated operating expenses related to the project from that revenue.

Discounted cash flow (DCF) valuation methods, including the net present value (NPV) and the internal rate of return (IRR) methods, are techniques that use time value of money concepts to measure the present value of cash inflows and cash outflows expected from an investment project.

The objective of the discounted cash flow (DCF) method is to focus the attention of management on relevant cash flows appropriately discounted to present value. The factors used to evaluate capital investments under discounted cash flow include the dollar amount of the initial investment, the dollar amount of future cash inflows and outflows, and the rate of return desired for the project.

The rate used to discount future cash flows may be set by management using several different approaches. Management may use a weighted average cost of capital (WACC) method, a specific target rate assigned to new projects, or a rate that relates to the risk specific to the proposed project. If the proposed project is similar in risk to the ongoing projects of the organization, WACC is appropriate because it reflects the market's assessment of the average risk of the organization's projects.

Discounted cash flow methods are widely viewed as superior to methods that do not consider the time value of money (e.g., the payback period method). However, discounted cash flow methods do have an important limitation—they frequently use a single interest rate assumption. This assumption is often unrealistic because, over time, as management evaluates its alternatives, actual interest rates or risks may fluctuate.

1.3 Financing Decisions

1.3.1 Short-Term Financing

A variety of short-term financial instruments, each with their own risk characteristics, are available to financial managers for various short-term financing needs. Short-term financing is generally classified as current and will mature within one year. Rates associated with short-term financing tend to be lower than long-term rates and presume greater liquidity on the part of the organization.

- **Trade Credit**

  Trade credit (accounts payable) generally provides the largest source of short-term credit for small organizations. Trade credit represents the purchases of goods and services as part of usual and customary business transactions that are generally paid 30 to 60 days after acquisition of the goods and services unless an early payment discount is offered.

- **Short-Term Bank Loans**

  Short-term bank loans are notes payable to financial institutions that are due in 12 months or less from the time of issuance. In addition to interest fees, lenders will also include other compensation in the form of fees.

© Becker Professional Education Corporation. All rights reserved.

- **Line of Credit**

  A line of credit is an arrangement with a financial institution that establishes a maximum loan amount that can be borrowed. The borrower can access and pay back funds at any time as long as the credit limit is not exceeded.

- **Commercial Paper**

  Commercial paper is unsecured, short-term debt issued by creditworthy organizations to finance payroll, accounts payable, inventory, and other short-term liabilities. Most commercial paper loans are sold at a discount, mature at par value, and have terms of no more than 270 days. Commercial paper is issued in denominations of $100,000 or more.

- **Banker's Acceptances**

  A banker's acceptance is a negotiable instrument that is similar to a postdated check, except that it is guaranteed by the bank rather than the account holder. Banker's acceptances can be used as a bank-backed payment for large transactions. After issuance, banker's acceptances can be traded at a discount in the money market.

- **Letters of Credit**

  A letter of credit represents a third-party guarantee (generally by a bank) of financial obligations incurred by an organization. Letters of credit can represent an external credit enhancement used by an organization issuing otherwise unsecured debt to enhance its credit. Alternatively, they can be required by a creditor to ensure payment.

1.3.2 Long-Term Financing

Organizations need larger amounts of funding to secure the purchase of long-term assets. Long-term financing includes long-term debt and equity financing that are considered larger in amounts and more permanent in nature. The long-term financing, including debt financing and equity financing, are referred to using the term capital structure and can include both external and internal funds such as:

- **External Funds**: The organization can obtain new external funds through the issuance of long-term bonds, preferred stock, and/or common stock.
- **Internal Funds**: The organization can also finance its operations by reinvesting the retained earnings that are profits accumulated in an organization over the years but are not yet distributed to shareholders in the form of dividends.

© Becker Professional Education Corporation. All rights reserved.

An organization typically uses a mix of debt and equity financing. Each has its advantages and disadvantages, as summarized below:

	Advantages	Disadvantages
Debt Financing	• Tax deductibility of interest payments. • Lower cost of capital relative to equity (due to the interest tax deduction and because there is less risk to the investor). • Low-security issuance costs (relative to equity). • No dilution of earnings per share (EPS) because no new shares are issued. • Flexibility to retire bonds if they are callable. If the bond is callable and market interest rates decline, the organization can call the bonds and replace them with lower-cost issues.	• Obligation to meet interest and principal payments as they come due. • Increased financial risk associated with payment obligations and a defined maturity date. • As debt increases, obtaining new debt is possible only at a higher cost because of the increased risk and increased financial leverage. • Negative impact on solvency ratios. • Issuance of debt may include some restrictive covenants; if violated, the organization is in technical default, and the debt is due immediately.
Equity Financing	• Flexibility regarding dividend payments, as they are not required. • Lower financial risk (relative to debt), as there is no loan to repay and no maturity date. • Issuing stock does not entail covenants that the issuer must adhere to. • Issuing equity securities improves the debt-to-equity ratio for the organization and, therefore, reduces the level of credit risk, which helps the organization obtain additional debt at a lower interest rate.	• No tax benefit for dividend payments because dividends are not tax-deductible. • Higher cost of capital (relative to debt). • High-security issuance costs (relative to debt), due to underwriting fees paid to investment banks. • EPS will be diluted because of new common shares issued. • Voting power of shareholders is also diluted.

© Becker Professional Education Corporation. All rights reserved.

1.4 Dividend Decisions

Dividend decisions are concerned with determining whether and how much of after-tax profit to pay out to shareholders in the form of dividends versus how much to retain in the retained earnings of the organization or to help fund the growth of the organization.

Pass Key

Internal auditors should understand finance concepts of the activity under review to help identify risks and controls that may relate to:

- Investment decisions
- Financing decisions
- Dividend decisions

2 Accounting Concepts

2.1 Overview of Accounting Concepts

The internal audit function may be asked to perform engagements that require an understanding of accounting, which can be differentiated between financial and managerial accounting. Most engagements relating to financial accounting and financial statements are usually performed by external auditors; however, internal auditors may be asked to support those engagements. Managerial accounting can be viewed more as an internal organizational activity used in organizational decisions. Therefore, it is important to understand accounting concepts to be able to identify risks and controls during engagement planning.

Accounting is the process of identifying, classifying, measuring, recording, and communicating in monetary terms transactions and events of an economic entity that are of a financial character and can be viewed as a framework for financial reporting.

2.1.1 Managerial Accounting

The internal audit function may be more involved in engagements related to managerial accounting, which can be described as internal financial reporting that is not as regulated as financial reporting. Managerial accounting is more flexible, and internal standards based on specific focus areas may be determined. Managerial accounting is used in internal decision making and is focused on the cost of various operations. However, many of the concepts that apply are the same as those in financial accounting.

2.1.2 Financial Accounting

Financial accounting focuses on identifying, recording, and communicating an organization's economic events, such as sales, payments, and cash collections, to interested parties. The primary goal of external financial reporting is to produce reliable and accurate financial statements that reflect the organization's activities. These events are systematically recorded as they occur in the accounting cycle to track the organization's financial activities and understand its use of funds.

© Becker Professional Education Corporation. All rights reserved.

The accounting cycle can be broken down into the following steps:

1. Identify and analyze events.
2. Journalize transactions.
3. Post transaction to the general ledger.
4. Prepare an unadjusted trial balance and working papers.
5. Record adjusting entries.
6. Prepare an adjusted trial balance.
7. Prepare the financial statements.
8. Prepare closing entries.
9. Prepare the post-closing trial balance.
10. Record reversing and adjusting entries.

The purpose of the accounting cycle is to ensure that all financial transactions are accurately recorded, processed, and summarized to produce reliable quarterly and annual financial reports. This process involves recording transactions in the general ledger, making necessary adjustments, and consolidating entries to prepare accurate financial statements. The transactions are usually recorded and maintained in an IT accounting system.

Auditors focus on the inputs, processes, and outputs of the cycle to identify risks and test controls. Since the accounting cycle is continuous, it repeats each period. Risks relating to financial accounting can be summarized using the two main categories of principles in the generally accepted accounting principles (GAAP) standards: recognition (recorded amounts) and disclosure of information that, if omitted, may be misleading to financial statement users.

The internal controls relating to financial reporting help to ensure accuracy and completeness of the organization's financial information and can address risks relating to valuation, existence, completeness, accuracy, presentation, and disclosure.

Pass Key

Risks and controls to consider during engagement planning relating to finance and accounting can include:

- Risks of erroneous valuation
- Incomplete disclosure
- Overstatement of assets
- Fraud (e.g., misrepresentation)
- Understatement (accuracy and completeness) of liabilities
- Accuracy of revenue recognition (risks of overstatement and understatement)
- Compliance with accounting standards and/or policies

© Becker Professional Education Corporation. All rights reserved.

2.2 Assets

During engagement planning, including for managerial accounting or operational engagements, internal auditors should understand the accounting concepts that may apply to the activity under review.

Assets represent probable future economic benefits obtained or controlled by a particular organization as a result of past transactions or events. Generally, assets are what an organization "owns." There are five categories of assets reported on the balance sheet:

- **Current Assets**: Cash and other assets expected to be converted to cash or consumed either within one year of the balance sheet date or within the organization's operating cycle, whichever is longer. Current assets are listed in order of liquidity. Examples: cash and cash equivalents, short-term investments (management ability and intent to sell within a year), accounts receivable, inventories, and prepaid expenses (receive benefit within one year).

  Common risks relating to current assets can include existence as well as valuation.

- **Investments and Funds**: Assets that are not used directly in operations. These are noncurrent because of management's intent to not convert the assets into cash within the next year or within the organization's operating cycle, whichever is longer. Examples: investments in equity and debt securities of other companies, land held for speculation, noncurrent receivables, certificates of deposit having a maturity date greater than one year from the date the certificate was issued, and cash set aside for special purposes.

  Investments can include held-to-maturity, available-for-sale, or trading accounting securities. Valuation of investments is often a challenge and risk for an organization and, therefore, understanding the risks and controls related to estimates and valuation is beneficial. Considerations when reviewing investments are the reliability of the valuation or estimate as well as the time frame of the investment.

- **Property, Plant, and Equipment (Fixed Assets)**: Assets that are tangible, long-lived, and used in business operations. Reported at historical cost less accumulated depreciation to date (except land, which is not depreciated). Examples: land, land improvements, buildings, equipment, machinery, furniture, and natural resources. Risks relating to fixed assets often relate to existence and valuation.

- **Intangible Assets**: Assets that have no physical substance, are long-lived, and used in the operations of the organization. These assets typically represent exclusive rights that an organization can use to generate future revenues. Reported at historical cost net of accumulated amortization (usually shown net). Examples: patents, copyrights, trademarks, trade names, and franchises.

  A common risk relating to intangible assets is improper valuation or recognition due to the subjectivity of the estimate. A common example of an intangible asset for the internal audit function's review is intellectual property (IP), such as a patent.

- **Other Assets**: A catch-all category of noncurrent assets. This category is reserved for assets that will not fit into one of the first four categories discussed above. Examples: long-term prepayments (sometimes called deferred charges) and deferred income taxes.

Each organization varies in terms of asset composition; therefore, the types of assets reported on each organization's balance sheet may differ.

© Becker Professional Education Corporation. All rights reserved.

2.2.1 Property, Plant, and Equipment (Fixed Assets)

There are additional accounting concepts related to fixed assets that are useful to understand and may help with the identification of risks, including those related to the valuation of fixed assets.

- **Depreciation:** The goal of a depreciation method should be to provide for a reasonable, consistent matching of revenue and expense by systematically allocating the cost of the depreciable asset over its estimated useful life.

  The actual accumulation of depreciation in the books is accomplished by using a contra-account, such as accumulated depreciation or allowance for depreciation.

  - Straight-Line Depreciation: Determined by the formula:

$$\frac{\text{Cost} - \text{Salvage value}}{\text{Estimated useful life}} = \text{Depreciation}$$

    Estimated useful life is usually stated in periods of time, such as years or months.

  - Units-of-Production (Productive Output or Activity Method) Depreciation

    The units-of-production method relates depreciation to the estimated production capability of an asset and is expressed in a rate per unit or hour.

$$\frac{\text{Cost} - \text{Salvage value}}{\text{Estimated units or hours}} = \text{Rate per unit or hour}$$

$$\text{Rate per unit (or hour)} \times \text{Number of units produced (or hours worked)} = \text{Depreciation expense}$$

  - Sum-of-the-Years'-Digits Depreciation

    The sum-of-the-years'-digits method is one of the accelerated methods of depreciation that provides higher depreciation expense in the early years and lower charges in the later years.

    To find the sum-of-the-years'-digits, each year is progressively numbered and then added. For example, the sum-of-the-years'-digits for a five-year life would be:

    1 + 2 + 3 + 4 + 5 = 15

    For four years: 1 + 2 + 3 + 4 = 10

    For three years: 1 + 2 + 3 = 6

    The sum-of-the-years'-digits becomes the denominator. The numerator is the remaining life of the asset at the beginning of the current year. For example, the first year's depreciation for a five-year life would be 5/15 of the depreciable base of the asset.

$$\text{Depreciation expense} = (\text{Cost} - \text{Salvage value}) \times \frac{\text{Remaining life of asset}}{\text{Sum-of-the-years' digits}}$$

© Becker Professional Education Corporation. All rights reserved.

When dealing with an asset with a long life, the general formula for finding the sum-of-the-years'-digits is:

$$S = \frac{N \times (N + 1)}{2}$$

Where:

N = Estimated useful life

- Declining Balance Depreciation

  The most common of these accelerated methods is the double-declining-balance method, although other alternative (less than double) methods are acceptable. Under double-declining balance, each year's depreciation rate is double the straight-line rate. In the final year, the asset is depreciated to its salvage value, if any. Double-declining-balance depreciation is calculated using the following formula, where n is the number of years of the asset's useful life:

$$\text{Depreciation expense} = 2 \times \frac{1}{n} \times (\text{Cost} - \text{Accumulated depreciation})$$

  No allowance is made for salvage value because the method always leaves a remaining balance, which is treated as salvage value. However, the asset should not be depreciated below the estimated salvage value.

- **Salvage Value:** Salvage or residual value is an estimate of the amount that will be realized at the end of the useful life of a depreciable asset. Frequently, depreciable assets have little or no salvage value at the end of their estimated useful life and, if immaterial, the amount(s) may be ignored in calculating depreciation.
- **Estimated Useful Life:** Estimated useful life is the period of time over which an asset's cost will be depreciated. It may be revised at any time, but any revision must be accounted for prospectively, in current and future periods only (change in estimate).

2.3 Liabilities

Liabilities represent probable future sacrifices of economic benefits arising from present obligations of a particular organization to transfer assets or provide services to other entities in the future as a result of past transactions or events. Liabilities represent what an organization "owes." Liabilities are reported as either current or non-current obligations.

- **Current Liabilities**: Represent obligations that are expected to be satisfied with current assets or the creation of other current liabilities. Includes all liabilities that are expected to be satisfied within one year or within the organization's operating cycle, whichever is longer. Examples: accounts payable, notes payable, unearned (or deferred) revenues, accrued liabilities, and current maturities of long-term debt.
- **Long-Term Liabilities**: Represent obligations that will not be satisfied within the next year or within the organization's operating cycle, whichever is longer. Examples: long-term notes, bonds, lease obligations, and pension obligations.

© Becker Professional Education Corporation. All rights reserved.

Some of the risks that may be identified relating to liabilities during engagement planning include the valuation of bonds, proper categorization of leases, valuation of pension obligations, and compliance with debt covenants.

Additionally, an organization may have a contingent liability, which is an event that may but is not certain to occur, such as pending litigation. A loss contingency that is probable and that can be reasonably estimated should be reflected in the accounts.

2.4 Stockholders' Equity (Retained Earnings)

Stockholders' equity (also called shareholders' equity) represents the shareholders' residual claim in the entity's assets after deducting liabilities (i.e., the difference between what the organization "owns" and what the organization "owes").

Equity is presented in order of preference upon liquidation. Stockholders' equity is generally presented on the statement of financial position (balance sheet) as the last major section, following liabilities. The categories on the balance sheet can be summarized by the accounting equation:

Assets = Liabilities + Stockholders' equity

or

Assets – Liabilities = Stockholders' equity

Categories of equity include paid-in capital, retained earnings, accumulated other comprehensive income, and treasury stock.

Additionally, other concepts related to equity include:

- **Contributed Capital:** Equity resulting from the contributions of owners, also known as paid-in capital.
- **Retained Earnings:** Accumulated net income (or losses) during the life of the organization that have not been paid out as dividends.
- **Dividends:** The distribution of part of a company's earnings to shareholders.

2.4.1 Capital Stock (Legal Capital)

Legal capital is the amount of capital that must be retained by the organization for the protection of creditors. Capital stock is valued at par, which refers to the value of issued shares.

Stock is divided into two classes, common and preferred. Generally, preferred stock is issued with a par value, but common stock may be issued with or without a par value. No-par common stock may be issued as true no-par stock or no-par stock with a stated value. Organizations may raise funds by selling common stock, preferred stock, or both.

- **Common Stock**

  Common stock is the basic ownership interest in an organization. Common shareholders bear the ultimate risk of loss and receive the ultimate benefits of success. Because common shareholders bear the risk of loss, they are not guaranteed dividends or a share of assets upon dissolution of the organization. Common shareholders generally control management through their right to vote. Common shareholders also have the right to share in the earnings of the organization and the right to share in assets upon liquidation after the claims of creditors and preferred shareholders are satisfied.

© Becker Professional Education Corporation. All rights reserved.

- **Preferred Stock**

  Preferred stock is an equity security with preferences and features not associated with common stock. Preferred stock may include a preference relating to dividends, which may be cumulative or noncumulative and participating or nonparticipating. Preferred stock may also include a preference relating to liquidation. Usually, preferred stock does not have voting rights.

2.4.2 Additional Paid-in Capital

Additional paid-in capital is generally contributed capital in excess of par value or stated value. It can also arise from many different types of transactions. Additional paid-in capital may be aggregated and shown as one amount on the balance sheet.

2.4.3 Treasury Stock

Treasury stock is an organization's own stock that has been issued to shareholders and subsequently reacquired (but not retired). Treasury stockholders are not entitled to any of the rights of ownership given to common shareholders, such as the right to vote or to receive dividends. In addition, a portion of retained earnings equal to the cost of treasury stock may be restricted and may not be used as a basis for the declaration or payment of dividends (depending on applicable state law).

2.4.4 Retained Earnings

Retained earnings (or deficits) are accumulated earnings (or losses) during the life of the organization that have not been paid out as dividends. The amount of accumulated retained earnings is reduced by distributions to stockholders and transfers to additional paid-in capital for stock dividends. Retained earnings do not include treasury stock or accumulated other comprehensive income. If the retained earnings account has a negative balance, it is called a deficit. The calculation of retained earnings can be summarized as:

Beginning retained earnings + Net income (or – Net loss) – Dividends = Ending retained earnings

2.4.5 Accumulated Other Comprehensive Income

Components of accumulated other comprehensive income include pension adjustments, unrealized gains and losses on available-for-sale debt securities and hedges, foreign currency translation adjustments, and any portion of a gain or loss that is the result of a change in credit risk of debt when the fair value option is elected.

These components of other comprehensive income are not included in determining net income and, therefore, are not included in retained earnings. Rather, these components are recognized in the period in which they occur and are combined with net income to determine comprehensive income. Total accumulated other comprehensive income must be shown in the shareholders' equity section separate from capital stock, additional paid-in capital, and retained earnings.

© Becker Professional Education Corporation. All rights reserved.

MODULE

6 Key Risks and Controls Related to Business Processes

Part 2
Unit 1

This module covers the following topics from the *CIA examination syllabus*:

CIA Syllabus—Section A: Engagement Planning

3. Plan the engagement to assess key risks and controls

   May include but is not limited to:

   f. When planning an engagement, recognize key risks and controls related to common business processes such as asset management, supply chain management, inventory management, accounts payable, procurement, compliance, third-party processes, customer relationship management systems, enterprise resource planning systems, and governance, risk, and compliance systems

1 Understanding Business Processes

Requirements **Standard 13.2 Engagement Risk Assessment (Excerpt)**

Internal auditors must identify the risks to review by:

- Identifying the potentially significant risks to the objectives of the activity under review.
- Considering specific risks related to fraud.
- Evaluating the significance of the risks and prioritizing them for review.

When internal auditors have identified the relevant risks for an activity under review in past engagements, only a review and update of the previous engagement risk assessment is required.

© Becker Professional Education Corporation. All rights reserved.

1.1 Business Processes

Business processes are typically organized into functional areas or departments such as human resources, procurement, product development, sales, marketing, production, finance, accounting, IT, and logistics. These processes may be managed internally, outsourced partially, or outsourced entirely. Managing processes in-house versus outsourcing them can introduce varying risks and control considerations. Some business processes are also treated as projects, requiring distinct management approaches.

Business processes often span multiple functional areas, requiring effective coordination and communication. They are designed to support the achievement of specific business objectives, with their sub-processes interconnected to create economies of scale through unified planning, direction, monitoring, and control.

The internal audit function analyzes business processes to understand their context, gather information, and identify risks. This assessment helps prioritize areas of higher risk and allocate internal audit resources accordingly.

1.2 Collect Information to Understand Business Processes

To determine the appropriate focus areas within the business process, internal auditors must first develop a thorough understanding of the business process and its context. This includes identifying the objectives of the activity under review and how they align with the organization's overall strategy, mission, and vision. Internal auditors should also consider the long-term strategies and annual goals established for the process.

To gain such understanding, internal auditors can review various forms of business process documentation, including:

- Previous engagement workpapers
- Process workflows (e.g., flowcharts) and organizational charts for the activity under review
- Job descriptions or related documents
- Customer reviews and feedback
- Plans and budgets for the process
- Policy and procedure manuals
- Trends in key performance indicators

Reviewing process workflows and accompanying narratives is particularly valuable. If no process flowchart is available, internal auditors can collaborate with the process owner to create one, often through walk-throughs. This exercise helps internal auditors understand how the different components of the process interconnect as well as the process's inputs and outputs.

Pass Key

Reviewing or creating process workflows is a crucial step toward a comprehensive understanding of the process. These workflows can demonstrate how one process or sub-process interacts with or impacts other processes from a risk and control perspective.

© Becker Professional Education Corporation. All rights reserved.

1.3 Documenting Business Processes

A business process should be documented, typically by the process owner and those involved in the process. Commonly used documentation methods include process maps, flowcharts, and process narrative memoranda.

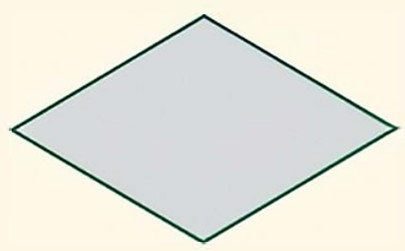
- **Process Map**

  Process maps are visual representations that outline the inputs, steps, workflows, and outputs of a process. They can be created at various levels of detail, ranging from high-level overviews to detailed activity-level maps. Process maps may also include accompanying narratives to provide additional context.

  There are no strict standards for the format or symbols used in process mapping. Process maps are generally organized to ensure clarity and logical progression so that the sequence of activities flows either from left to right or top to bottom.

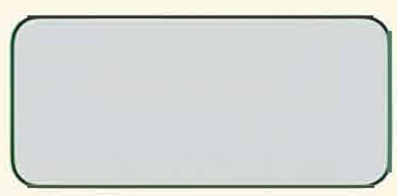
Illustration 1 Common Process Mapping Symbols

Process or operation—indicating a process, subprocess, or activity



Decision—indicating alternative choices resulting in different flows or activities

Flow line—indicating the direction of activities and workflows



Terminator—indicating the start or end of a flow

- **Flowcharts**

  A flowchart is a symbolic diagram representing the sequential flow of authority, processes, and documents. General rules for flowchart organization include:

  - Show the general flow of documents and data.
  - Start at the top of the page and move from top to bottom and from left to right.
  - Use descriptive wording familiar to the reader.
  - Avoid intersecting flow lines by using off-page/on-page connectors.

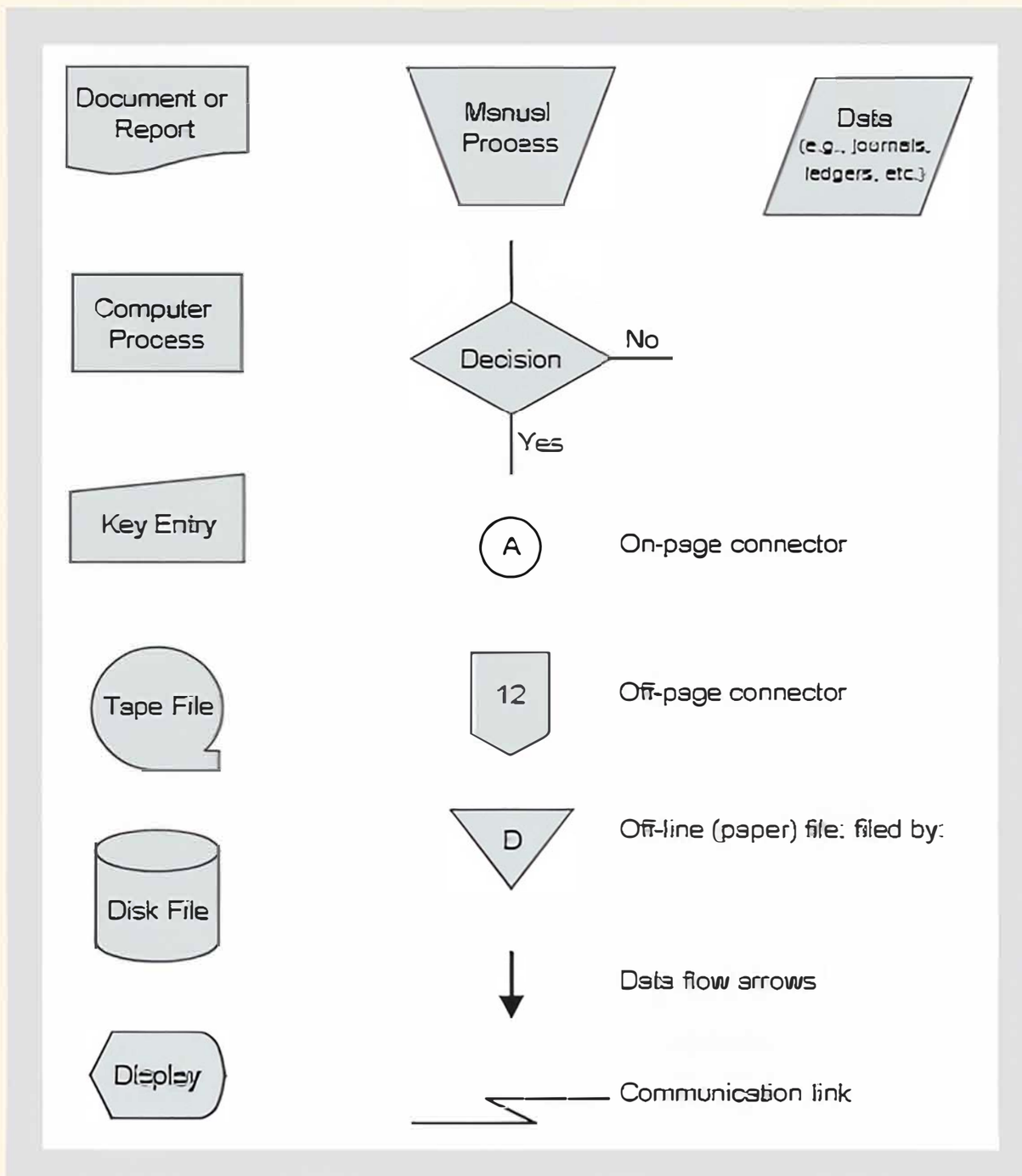
© Becker Professional Education Corporation. All rights reserved.

A high-level flowchart can be used to illustrate broad inputs, tasks, workflows, and outputs, facilitating the understanding of the overall activities, systems, reports, and interfaces with other processes or subprocesses. To document specific inputs, tasks, actions, systems, decisions, and outputs, detailed flowcharts can be used. Detailed flowcharts offer a more comprehensive depiction of the process flow and include additional information that enhances process understanding. These flowcharts may incorporate some or all of the following elements:

- **Key Risks:** Represented by symbols that highlight points in the process where failures could occur, potentially causing the process to not operate as designed.
- **Key Controls:** Identified using symbols to denote tasks, actions, or decisions that are critical to ensure that the process is adequately designed and operates effectively.
- **Individuals or Roles:** Indicating the individuals or positions responsible for performing key tasks or making decisions.
- **Timing:** Specifying when key tasks, actions, or decisions occur.
- **Elapsed time:** Highlighting the time required to complete specific tasks or decisions, which can be especially useful when assessing process efficiency.

Illustration 2 Common Flowchart Symbols

The symbols shown below represent the most commonly used symbols in flowcharts:



© Becker Professional Education Corporation. All rights reserved.

Pass Key

Flowcharts can best be used to help visualize all steps and actions in the business process, whereas an advantage of process maps is that they can be used to visualize all inputs, outputs, suppliers, and items needed to be completed within a process.

Process Narrative Memoranda

Narrative memoranda can be prepared to provide information about the process flow using written words only. The following are characteristics of situations where it is more appropriate to document a process using narrative write-ups:

- **Simplicity of the Process:** When the process is straightforward, a flowchart may not add significant value.
- **Complexity of Steps:** If the steps are highly detailed or complicated, narrative descriptions may be better suited to effectively capture the information than the limited space in flowchart symbols.
- **Preference of the Process Owner:** The process owner may prefer narrative documentation, especially if it aligns with or supports other process documentation.
- **Efficiency:** Narrative write-ups may be a faster and more practical way to document the process.

It is also common to create a hybrid format of documentation by combining flowcharts with supplementary narrative information. Compared with other methods, a hybrid documentation can provide the level of information necessary to understand processes in detail.

2 Internal Control Overview

Internal control is a process that is designed and implemented by an organization's management, board of directors, and other employees to provide reasonable assurance that the organization will achieve its operating, reporting, and compliance objectives.

2.1 Internal Control Categories

Internal controls can function as preventive controls, detective controls, safeguarding controls, and/or physical controls.

2.1.1 Preventive Controls

Preventive controls are proactive measures implemented prior to an action, event, or transaction in order to prevent errors or fraud when those actions, events, or transactions occur. Preventive controls are generally the most effective. Strong, preventive controls will keep invalid transactions from being processed and assets from being misappropriated. Each organization should tailor these preventive controls to its specific operational and industry needs.

Preventive controls over financial reporting are designed to provide reasonable assurance that only valid transactions are recognized, approved, and submitted for processing. Most preventive controls are applied before the processing activity occurs.

© Becker Professional Education Corporation. All rights reserved.

Examples of preventive controls include the following:

- Employee screening and periodic fraud policy training
- Segregation of duties
- Access control by using passwords and multi-authentication tools
- Physical controls over an organization's assets and cataloging usage
- Administrative controls, such as documenting policies and procedures and monitoring for updates as needed

2.1.2 Detective Controls

Detective controls are designed to provide reasonable assurance that errors or irregularities are discovered and corrected on a timely basis. Detective controls over financial reporting are normally performed after the record-keeping processing for a transaction has been completed.

Examples of detective controls include the following:

- Reviewing financial performance such as budget to actual data
- Conducting a physical inventory count
- Performing a reconciliation of accounts such as fixed assets and cash

2.1.3 Safeguarding Controls

Safeguarding controls limit access to authorized personnel only. This access includes both direct or physical access to assets and indirect access such as through the authorization to acquire, use, or dispose of assets.

Examples of safeguarding controls for cash and related accounts include the following:

- Lockbox system for collecting cash receipts from customers
- Direct deposit of pay in lieu of the distribution of physical paychecks or cash to employees
- Write-offs of uncollectible accounts only by the credit department manager

2.1.4 Physical Controls

Physical controls for safeguarding assets involve security devices and limited access to programs and restricted areas, including computer facilities. Physical controls include:

- Physical segregation and security of assets, protective devices, and bonded or independent custodians (e.g., banks, safe deposit boxes, lock boxes, and independent warehouses).
- Authorized access to assets and records (such as through the use of computer access codes, prenumbered forms, and required signatures on documents for the removal or disposition of assets).
- Periodic counting and comparison of actual assets with amounts shown in accounting records (e.g., physical counts and inspections of assets, reconciliations, and user review of computer-generated reports).

© Becker Professional Education Corporation. All rights reserved.

2.2 Relevant Assertions

When determining the risks and controls within an accounting or financial reporting process, the relevant assertion level for each significant account balance, transaction class, and disclosure can help assist with this analysis. Assertions are similar to objectives, and process controls are designed to mitigate the risk that the objectives (or assertions) may not be met.

2.2.1 Assertions

There are six main financial statement assertions:

1. **Completeness**

   All account balances, transactions, and disclosures that should have been recorded have been recorded and included in the financial statements.

2. **Cutoff**

   Transactions have been recorded in the correct (proper) accounting period.

3. **Valuation, Allocation, and Accuracy**

   Account balances, transactions, and disclosures are recorded and described fairly and measured at appropriate amounts, and any resulting valuation or allocation adjustments are appropriately recorded.

4. **Existence and Occurrence**

   Account balances exist, and transactions that have been recorded and disclosed have occurred and pertain to the organization.

5. **Rights and Obligations**

   The organization holds or controls the rights to assets, and liabilities are the obligations of the organization.

6. **Understandability of Presentation and Classification**

   Transactions have been recorded in the proper accounts and appropriately aggregated or disaggregated. Financial information is appropriately presented and described, and disclosures are clearly expressed and understandable in the context of the applicable financial reporting framework.

3 Asset Management

3.1 Cash and Cash Equivalents Management

3.1.1 Overview

Factors influencing the levels of cash include the volume of collections and their timing, the volume of disbursements and their timing, and the degree to which idle cash is invested in marketable securities.

Organizations use various techniques to maximize cash balances, including managing float, synchronizing cash inflows and outflows, speeding collections and deposits, and mitigating risks with overdraft systems or compensating balances.

© Becker Professional Education Corporation. All rights reserved.

Organizations hold cash to make routine payments for business transactions, to repay loans and other financing costs, to maintain compensating balances for banks, to prepare for future uncertainties, and to prepare for future opportunities. Motives for holding cash include:

- **Transaction Motive**: An organization may hold cash to meet payments arising from the ordinary course of business.
- **Speculative Motive**: Cash may be needed to take advantage of temporary opportunities.
- **Precautionary Motive**: It is important to have enough cash on hand to maintain a safety cushion to meet unexpected needs.

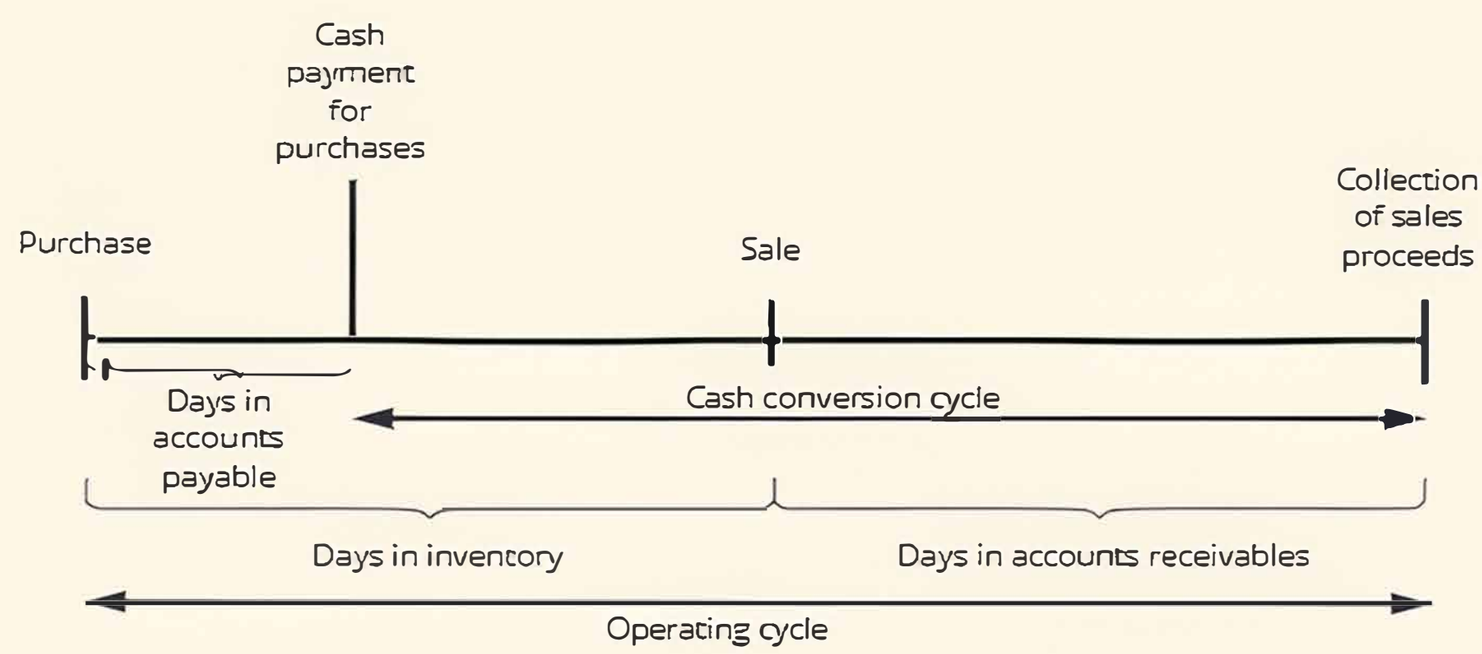
Maintaining high levels of cash can be a disadvantage because of:

- The "negative arbitrage" effect (i.e., interest obligations exceed interest income from cash reserves).
- Increased attractiveness as a takeover target.
- Investor dissatisfaction with allocation of assets (i.e., failure to pay dividends).

3.1.2 Operating Cycle and Cash Conversion Cycle

Either speeding up cash inflows or slowing down cash outflows increases cash balances. Improved cash inflows are generally achieved through faster accounts receivable collections. Reduced cash outflows are often achieved through delayed (or deferred) disbursements. The combination of current cash inflows and current cash outflows related to an organization is called the operating cycle. The objective of financial managers is to shorten the operating cycle.

Illustration 3 Operating and Cash Conversion Cycles



© Becker Professional Education Corporation. All rights reserved.

3.1.3 Key Risks and Controls Related to the Cash Cycle

- **Fraud Risk:** Cash is an area with high fraud risk, especially when the system of internal control is weak. Lapping and kiting are two common cash fraud schemes.
  - **Lapping:** The theft of cash is often concealed by failing to account for cash receipts. The most common of these methods is known as lapping. Lapping occurs when an employee withholds funds received by a customer for personal use and fails to apply these receipts of cash or checks to the customer's receivable balance. The unrecorded receipt is covered by applying a subsequent receipt to the previously unrecorded account.

    Safeguards against lapping include the following:

    — Independent comparison of recorded cash receipts with funds actually deposited.

    — Separation of incoming receipts from subsidiary accounts receivable remittance advice.

    — Comparison of the details of bank deposits and the details of remittance credits.

    — Provision of timely statements.

    — Confirmation of customer balances.

    One of the best methods to guard against lapping is the use of a "lock box" system. In this system, customers send their payments directly to the bank, which prevents an organization's employees from having access to payments received. A statement is then sent by the bank to the organization so the cash can be applied in the general ledger to the outstanding receivable balance.
  - **Kiting:** Kiting occurs when a check drawn on one bank is deposited in another bank and no record is made of the disbursement in the balance of the first bank until after year-end. Kiting may be used to cover a cash shortage or to pad an organization's cash position. Kiting results in an intentional overstatement of cash in the financial statements as the cash is simultaneously reflected in two different bank accounts.

    To detect kiting effectively, a bank transfer schedule should be prepared. For any bank-to-bank transfers that occur near year-end, the disbursement date on the check and in the ledger for the disbursing account should precede the receipt date noted by the bank and in the ledger for the receiving account.

    To ensure that kiting has not occurred, evidence should exist that all deposits in transit and outstanding checks listed on the bank reconciliation at year-end cleared in the next period. This information can be confirmed by using a bank cutoff statement.
- **Segregation of Duties:** Segregation of duties is a key control over cash. Proper segregation of duties demands that close consideration be given to check-writing authority. Separation of cash handling, record keeping, and reconciliation of bank statements should exist, as well as separation of petty cash activities. A strong system of internal control for cash would also include the use of a voucher system for cash disbursements.

© Becker Professional Education Corporation. All rights reserved.

3.2 Accounts Receivable Management

3.2.1 Overview

Accounts receivable management includes achieving a balance between converting accounts receivable into cash quickly to meet short-term obligations and extending enough credit to capture additional sales without increasing bad debt expense.

The factors that influence the level of receivables are:

- **Total Sales:** Higher sales generally mean higher receivables.
- **Level of Credit Sales:** Receivables are higher for organizations that primarily sell on credit rather than cash.
- **Credit Policies:** Organizations with less stringent credit policies, including lower credit standards and longer payment periods, generally have higher receivables, but may also have higher write-offs.

3.2.2 Credit Policy

Credit policy is one of the major determinants of demand for an organization's products or services, along with price, product quality, and advertising. The credit policy of an organization is typically established by a committee of senior executives. Credit policy variables include:

1. **Credit Period:** Credit period is the length of time buyers are given to pay for their purchases. A commonly used credit period is 30 days. If the credit period is too long, the organization may experience cash shortages. A credit period that is too short may damage relationships with customers and negatively affect future sales.
2. **Credit Standards:** Credit standards refer to the required financial strength of credit customers. Extending credit to only financially strong customers minimizes uncollectible receivables, but also limits potential sales. Extending credit to a broader base of customers increases sales, but adds risk in that a greater percentage of receivables are likely to be written off.
3. **Collection Policy:** Collection policy is measured by an organization's stringency or laxity in collecting delinquent accounts. This is also a balancing act between wanting to collect cash owed quickly versus maintaining positive relationships with customers.
4. **Discounts:** Discounts include the discount percentage and period. Offering discounts to customers who pay early may result in faster receivables collection, depending on the terms of the discount and the customer's own cash needs and capacity to pay early.

3.2.3 Methods to Speed Collections

- **Customer Screening and Credit Policy:** An organization can choose to extend credit to more responsible customers, who are more likely to pay bills promptly.
- **Prompt Billing:** Timely billing of charges to credit customers ultimately serves to speed collections.
- **Payment Discounts:** Offering payment discounts may influence customers to pay faster and can result in improved cash collections. Discounts foregone represent a higher cost to the customer than a bank loan for similar financing.

© Becker Professional Education Corporation. All rights reserved.

- **Expedite Deposits:** Financial managers not only must collect credit sales in a timely manner, but also must ensure that funds are deposited and credited to their account quickly. The following techniques reduce the time during which payments received by an organization remain uncollected (not yet credited as cash in the bank).
  - **Electronic Funds Transfer:** The electronic movement of funds from one institution to another is called electronic funds transfer, or EFT. Electronic funds transfer and credit cards ensure timely payment. Having funds sent electronically to an organization's bank account facilitates immediate collection rather than waiting for checks to be deposited.
  - **Lockbox Systems:** Lockbox systems expedite cash inflows by having a bank receive payments from an organization's customers directly via mailboxes to which the bank has access. Payments that arrive in these mailboxes are deposited into the organization's account immediately.
- **Concentration Banking:** Concentration banking is characterized by the designation of a single bank as a central depository. Advantages of concentration banking include:
  - Improved controls over inflows and outflows of cash
  - Reduced idle balances
  - Improved effectiveness for investments
- **Factoring:** Factoring accounts receivable entails turning over the collection of accounts receivable to a third-party factor in exchange for a discounted short-term loan. Cash is collected from the factor immediately rather than from the customer according to the credit terms.

3.2.4 Key Risks and Controls Related to Accounts Receivable

- **Fraud Risk:** Common accounts receivable frauds include overstatement of receivables, achieved by overstating balances, reporting fictitious balances, or understating the allowance for uncollectible accounts.
- **Uncollectible Receivables:** An aging schedule is prepared and sent to the credit department for use in carrying out its collection program. At some point, receivables deemed uncollectible should be written off. Controls for writing off receivables include proper authorization (by the treasurer) and record keeping. Without proper control, amounts subsequently collected easily could be misappropriated by employees.
- **Sales Returns:** Returned goods must be examined to ensure that they correspond with the reason for return before credit is given. A serially numbered receiving report may be used as a sales return slip. Once the return is approved, the sales return is recorded and the related outstanding receivable is eliminated. Credit memos should not be prepared by individuals who collect or receive cash payments on accounts receivable; to do so would be an inadequate segregation of duties.
- **Sales Discounts:** Sales discount procedures and records should be reviewed to ensure that discounts are properly given and recorded based on the selected method (gross versus net). This ensures that receivables are not overstated.

© Becker Professional Education Corporation. All rights reserved.

3.3 Inventory Management

3.3.1 Overview

Inventory may represent the most significant current noncash resource of an organization. Inventory typically is most significant in organizations that involve the sale or manufacture of goods. Inventory may be classified as raw materials, work-in-process, and finished goods.

- **Raw Materials:** Inventory held for use in the production process.
- **Work-in-Process:** Inventory in production but incomplete.
- **Finished Goods:** Production inventory that is complete and ready for sale.

3.3.2 Inventory Management Strategies

- **Factors Influencing Inventory Levels**

  Inventory depends on the accuracy of sales forecasts. Lack of inventory can result in lost sales, and excessive inventory can result in burdensome carrying costs, including:

  - Storage costs
  - Insurance costs
  - Opportunity costs of inventory investment
  - Lost inventory due to obsolescence or spoilage

- **Optimal Levels of Inventory**

  Numerous factors affect the optimal level of inventory, including the usage rate of inventory per period of time, cost per unit of inventory, cost of placing orders for inventory, and the time required to receive inventory. Concepts related to the determination of the optimal level of inventory include:

  - Inventory turnover
  - Safety stock
  - Reorder point
  - Economic order quantity
  - Materials requirements planning

- **Safety Stock**

  Many organizations maintain safety stock to ensure that manufacturing or customer supply requirements are met. The determination of safety stock depends on the following factors:

  - Reliability of sales forecasts
  - Possibility of customer dissatisfaction resulting from back orders
  - Stockout costs (the cost of running out of inventory), including loss of income, the cost of restoring goodwill with customers, and the cost of expedited shipping to meet customer demand
  - Lead time (the time that elapses from the placement to the receipt of an order)
  - Seasonal demands on inventory

© Becker Professional Education Corporation. All rights reserved.

- **Reorder Point**

  The reorder point is the inventory level at which an organization should order or manufacture additional inventory to meet demand and to avoid incurring stockout costs.

- **Economic Order Quantity**

  When managing inventory, there is a trade-off between carrying costs (the costs of holding inventory) and ordering costs (the costs of ordering additional inventory). For example, if the order quantity is small then carrying costs are low, but inventory must be ordered more frequently to meet demand, which increases ordering costs.

  Ordering costs typically represent the costs of labor associated with order placement. The costs are driven by order frequency (rather than quantity per order) and they include the costs of entering the purchase order, processing the receipt of the inventory, inspecting the inventory to ensure that the goods received (typically a sample) are acceptable, and processing of the vendor invoice and consequent payment.

- **Just-in-Time Inventory Models**

  The *just-in-time (JIT) inventory model* was developed to reduce the lag time between inventory arrival and inventory use. JIT ties delivery of components to the speed of the assembly line. JIT reduces the need of manufacturers to carry large inventories but requires a considerable degree of coordination between manufacturer and supplier. The benefits of JIT implementation include tying production scheduling with demand, more efficient flow of goods between warehouses and production, reduced setup time, and greater employee efficiencies.

- **Kanban Inventory Control**

  Kanban inventory control techniques give visual signals that a component required in production must be replenished. This technique prevents oversupply or interruption of the entire manufacturing process as the result of lacking a component.

- **Computerized Inventory Control**

  Computerized inventory control operates by establishing real-time communication links between the cashier and the stock room. Every purchase is recognized instantaneously by the inventory database, as is every product return. Computers are programmed to alert inventory managers as to reorder requirements. In some cases, organization databases interface directly with supplier software to allow for instantaneous reorders, thereby removing the human element.

3.3.3 Key Risks and Controls Related to Inventory

- **Inventory Sales**

  - **Fraud Risk:** Common sales frauds include fictitious sales, failure to record sale returns, side agreements used to alter sales terms and conditions to induce customers to accept goods and services they otherwise do not need, and channel stuffing achieved by convincing distributors to purchase more inventory than they can sell in the near term.

  - **Segregation of Duties:** In a strong system of internal control for inventory sales, segregation of the functions in a sales transaction should exist as follows:

    1. **Preparation of the Sales Order**

       The sales function begins with the receipt of a customer purchase order by the sales department. If it is determined that the order can be filled, a serially numbered sales order is prepared and sent to the credit department for approval.

© Becker Professional Education Corporation. All rights reserved.

2. **Credit Approval**

   The credit department determines whether or not the customer may receive goods on credit. If the order is approved, a copy of the approved sales order is sent to the shipping department, the billing department, and the accounting department.

3. **Shipment**

   In the shipping department, a serially numbered bill of lading is prepared and a copy is sent to the customer. The goods are shipped, and at this point a receivable is created based on invoice shipping terms.

4. **Billing**

   The billing department prepares a serially numbered sales invoice. Shipping documents, sales orders, and invoices are compared to ensure that all shipments are based on valid customer orders and are properly billed. Prices and discounts are applied to the invoice, and necessary extensions and footings are computed. The invoice is then sent to the customer and to the accounts receivable department.

5. **Accounting**

   The sale is entered into the sales journal, and a receivable is recorded.

- **Inventory Held by the Organization**

  For inventory held by the organization, a proper system of internal control includes adequate safeguarding of inventory and proper segregation of duties. The following duties should be segregated:

  1. **Purchasing**

     Serially numbered, properly approved purchase orders should be prepared and issued to the accounting and receiving departments.

  2. **Receiving**

     The receiving department is solely responsible for the receipt of goods. This department is responsible for the verification of quantities received, detection of damaged goods, preparation of a receiving report, and delivery of goods received to the warehouse department. The receiving department should receive a copy of the purchase order that does not indicate the quantity ordered, so the receiving department is forced to count the goods upon arrival.

  3. **Warehouse**

     The warehouse department acts as custodian for the verified quantity of goods received.

  4. **Shipping**

     The shipping department is responsible for the shipment of goods after authorization (in the form of an approved sales order from the credit department).

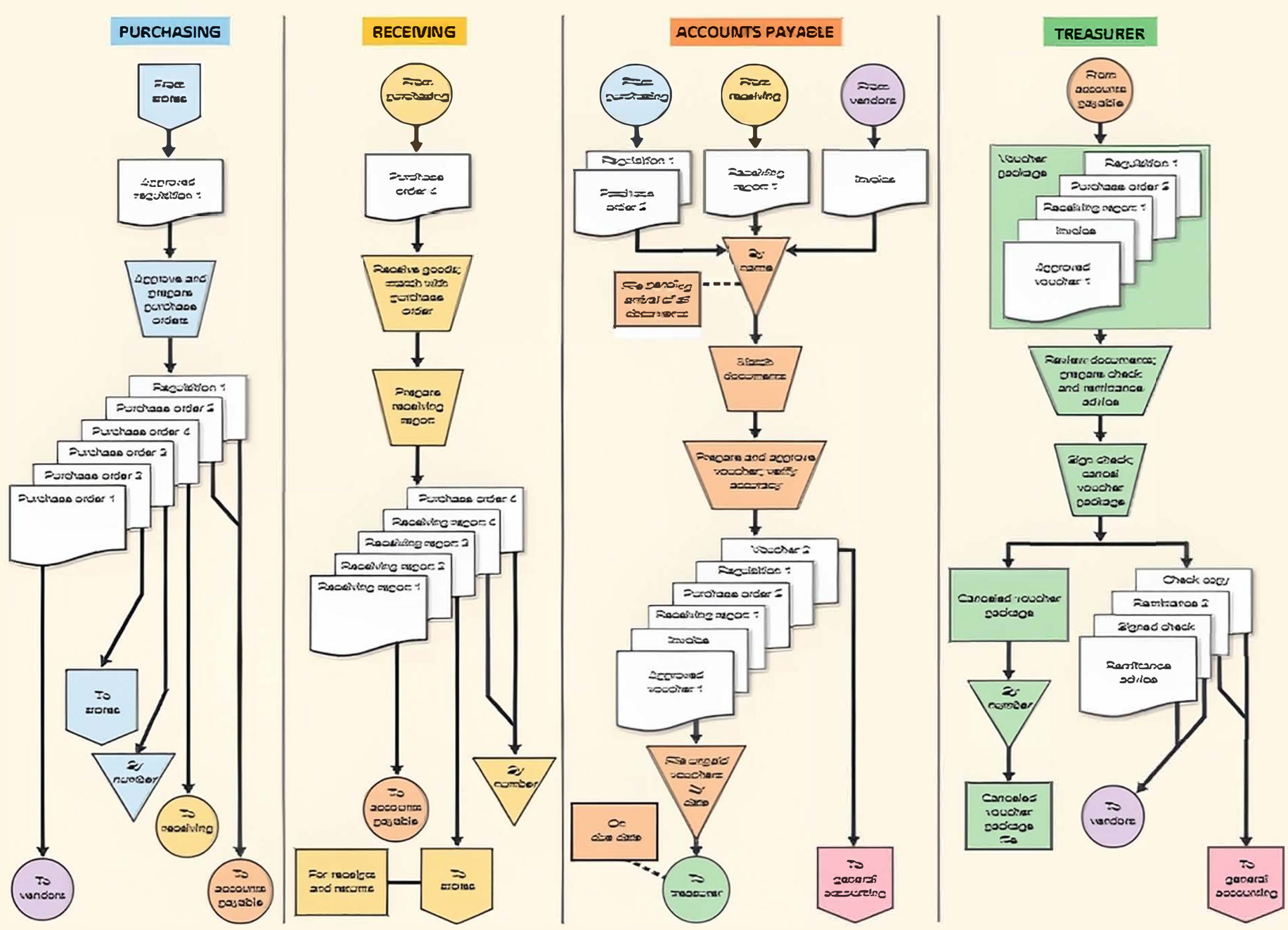
© Becker Professional Education Corporation. All rights reserved.

4 Procurement and Accounts Payable Management

4.1 Procurement Process

Procurement is the process of acquiring goods or services by an organization from external parties. The procurement process generally involves identifying organizational needs, sourcing suppliers, negotiating contracts, receiving goods and services, and making payments. The procurement process needs the attention of the internal audit function because of critical risks embedded in the purchasing process, as well as in the payment process pertaining to accounts payment management.

Illustration 4 Procurement and Accounts Payable Process



4.1.1 Key Risks Related to Procurement

- **Fraud and Corruption Risk:** Common fraud and corruption risks include fictitious invoice payments, kickbacks resulting in padded or non-competitive bids that are accepted, rigged bidding or tender processes, nonexistent or falsified due diligence, cost estimates that are not aligned with market rates, requirements prepared by a service provider solely to reduce competition, and bids being unsealed before the bid opening session.

© Becker Professional Education Corporation. All rights reserved.

- Other risks include:
  - **Conflicts of Interest and Bias:** This includes bias in procurement decisions and conflicts of interest among bid evaluators.
  - **Misaligned Procurement:** Procurement processes are not aligned with the organization's overall strategy.
  - **Breaches of Confidentiality:** The anonymity of bidders/tenderers and the confidentiality of bid information are not maintained.
  - **Lack of Transparency:** Selection and award criteria should be clearly and comprehensively disclosed.
  - **Unfair Bidding Processes:** Requests for proposals/invitations to tender are not widely distributed/advertised with sufficient time allowed for bidding.
  - **Supplier Misrepresentation:** Suppliers are not qualified, or falsify certifications, insurance documents, or other credentials.

4.1.2 Controls Related to the Procurement Process

- **Segregation of Duties**

  The following three functions in a purchase transaction should be segregated:

  1. **Purchase Requisition**

     The purchase requisition begins the purchasing cycle. The department in need of the asset or services sends a properly approved, serially numbered requisition to the purchasing department. The requisitioning department should not have the authority to actually place the purchase order. This would indicate a weakness in the system of internal control.

  2. **Purchase Orders**

     Prior to placing the order, the purchasing department should request bids from various suppliers to make sure that the best price is obtained. Once properly approved, the purchasing department should create the purchase order, which will indicate the description, quantity, and related information for the goods and services that are being requested. For control purposes, it is best that prenumbered purchase orders be used.

     There should be multiple copies that will be sent to: (i) the requisitioning department; (ii) the vendor; (iii) the receiving department; and (iv) the accounting department. If the purchase order is canceled, all copies should be recalled and filed so that every purchase order number is accounted for.

  3. **Receipt of Goods or Services**

     The copy of the purchase order sent to the receiving department serves as an authorization to accept the goods or services when they arrive. It is preferable that the copy not indicate the quantity ordered so that the receiving department is forced to count the goods upon arrival. In addition, the description of the goods should be matched to the purchase order and the condition of the goods should be examined. A receiving report is prepared by the receiving department and forwarded to the accounting department. The goods are forwarded to the requisitioning department.

© Becker Professional Education Corporation. All rights reserved.

- **Controls Over Cash Disbursements**

  Ideally invoices should be paid by check. For effective controls, the functions of approving the payment and signing the checks should be segregated. Approved voucher packets (matched invoice, purchase order, receiving report, and requisition) prepared by the accounting department (accounts payable) are received by the treasurer, who prepares, signs, and mails the checks and cancels all supporting documents after payment. Paid vouchers are returned to the accounting department for posting of the payment and filing of the documents.

- **Other Procurement Controls**
  - Maintain a robust vendor information system with strong access controls.
  - Establish a process for prequalifying suppliers and maintaining an updated list of approved vendors.
  - Provide a formal mechanism for suppliers to submit complaints or appeals regarding irregularities in the procurement process.
  - Regularly evaluate supplier performance based on objective criteria.
  - Conduct due diligence and background/affiliation checks on all individuals involved in the procurement process, including bid evaluators, procurement professionals, supervisors, and suppliers.
  - Systematically review winning and non-winning bids to detect any signs of bias, fraud, or corruption.

4.2 Accounts Payable Management

4.2.1 Overview

Accounts payable (or trade credit) generally provides the largest source of short-term credit for small organizations. Trade credit represents the purchases of goods and services as part of usual and customary business transactions for which payment is made 30 to 45 days after acquisition.

Although extension of payments under trade credit arrangements can be very effective in preserving cash balances and financing current operations, the effective annual interest cost can be extremely high if discounts are offered and foregone as part of this working capital management strategy.

There can be a high cost associated with a customer not taking advantage of a discount offered by the vendor. The decision whether or not to pay early and take the discount depends on several factors, including whether:

- The organization has the cash on hand to pay that particular vendor early.
- The organization wants to preserve its cash position for other purposes (investments, projects, maintaining a reserve, etc.).
- There is potential to negotiate even more favorable terms with vendors, including greater discounts or longer discount periods.

© Becker Professional Education Corporation. All rights reserved.

Organizations need to find an optimal balance between conserving cash and ensuring that vendors are paid in a timely manner. If an organization is a regular buyer and/or a large volume buyer from a particular vendor, it may be able to negotiate more favorable terms in order to either take advantage of discounts or extend payment periods. If, for example, the discount period is 10 days, an organization will want to pay on the 10th day. If the overall payment is due in 30 days and the discount is not taken, the organization should pay on the 30th day. Setting up automatic payments to pay vendors at the end of the payment period is ideal, as it allows the organization to conserve cash as long as it can and still pay in a timely manner.

4.2.2 Controls Related to Accounts Payable

Once the accounting department obtains the receiving report, it will record the payable, approve the invoice for payment, and record the payment after it is paid by the treasurer.

1. **Recording the Payable**

   The copy of the purchase order sent to the accounting department notifies it that there will be a future cash disbursement. The receiving report is compared with the purchase order and the vendor's invoice to confirm quantity and to prevent payment of charges for goods in excess of those ordered and received. The accounting department records the goods as received in inventory, and records a payable.

2. **Approving Invoice for Payment and Recording Payment**

   When the invoice arrives, the accounting department approves it by matching the invoice, purchase order, receiving report, and (sometimes) the requisition. When payment is made, the payable is reversed. The accounting department should ensure that the invoice amount is correct, and that it accurately reflects any purchase discounts or returns, before approving it for payment.

5 Compliance

5.1 Overview

Compliance is defined as adherence to laws, regulations, contracts, policies, procedures, and other requirements. This includes laws and regulations from authoritative bodies outside the organization, for example, the Environmental Protection Agency (EPA) or the Internal Revenue Service (IRS). Contracts, policies, and procedures may originate from inside the organization or from agreements entered into voluntarily. For example, a sales contract may stipulate certain product quality standards.

Aside from compliance with operational requirements, many organizations will engage with reporting requirements (e.g., SOX, PCI, HIPAA, or GDPR). Emerging/potential areas of regulatory compliance include sustainability reporting and the use of artificial intelligence.

Management takes on second line responsibilities related to compliance, although these roles may be blended with operational first line roles. Due professional care requires that internal auditors consider the probability of noncompliance.

© Becker Professional Education Corporation. All rights reserved.

5.2 Key Risks and Controls

5.2.1 Risks

The key compliance risk in organizational processes is noncompliance. Downstream consequences for noncompliance may vary depending on the unmet requirements, but these consequences can have a material impact on the achievement of organizational objectives.

Stakeholders (e.g., customers, employees, the local community, investors, etc.) are vulnerable to the consequences of organizational noncompliance. Noncompliance can result in direct financial impacts, such as fines and penalties, or reputational damage, which may result in indirect financial impacts.

Specific noncompliance risks can be assessed using a variety of measurement categories listed in the COSO: *Compliance Risk Management: Applying the COSO ERM Framework*, published in 2020:

- Legal—Consisting of civil and criminal fines and penalties.
- Financial—Internal and external costs associated with investigating and remediation (e.g., legal fees, consultants, investigators).
- Operational—Potential disruption of business operations from plant shutdowns, suspensions, debarments, and loss of license.
- Reputation (image)—Effect of media coverage; damage to the organization's image/brand; and subsequently diminished attractiveness to current and potential future employees, business partners, vendors, and customers.
- Health and safety—Employee, patient, customer.
- Ability to pursue strategic goals—Prohibition to added new customers, loss of license.

5.2.2 Controls

The COSO 2013 *Internal Control–Integrated Framework* (the framework) shows compliance as one of the three primary objectives of internal control, alongside reporting and operations. All five components of internal control (control environment, risk assessment, control activities, information and communications, and monitoring) are responsive to the compliance objective. As such, typical preventive and detective control approaches may be used to mitigate the risk of noncompliance.

Although the organization is held responsible for violations, perpetrators of noncompliance are often individuals, so controls such as segregation of duties, policies, procedures, checklists, access controls, and management review are appropriate. Governance and oversight controls, such as compliance committees, can offer additional support. Organizational culture plays an integral role in compliance management, and the U.S. Federal Sentencing Guidelines recommend having a separately identified compliance and ethics program.

© Becker Professional Education Corporation. All rights reserved.

5.2.3 Compliance and Ethics Program

Compliance and ethics (C&E) programs aim to pursue value creation for the organization through compliance with relevant requirements. Effective C&E programs contain several elements including:

- Standards and procedures.
- Governance, oversight, and authority.
- Due diligence in the delegation of authority.
- Communication and training.
- Monitoring, auditing, and reporting systems.
- Incentives and enforcement.
- Response to wrongdoing.

Organizations may create compliance departments to produce the C&E program. Ideally, these departments are separate from the legal and regulatory affairs departments.

C&E programs may not always be comprehensive in their coverage of compliance risks. For example, the risk of violating the Dodd-Frank Act may fall clearly within the scope of a company's C&E program. However, compliance with accounting standards required in filings with the U.S. Securities and Exchange Commission may be addressed within the accounting function and outside the scope of the C&E program. Management is responsible for following the program (with the management of specific departments being responsible for compliance concerns outside of the C&E), and the board is responsible for providing related oversight.

6 Third-Party Processes

6.1 Overview

When third parties fail to deliver or break down entirely, the damage to their clients' reputation and operations can often match or exceed the harm to the third party. Relying on third-party suppliers or service providers changes an organization's risk profile. While "third party" typically refers to significant projects (e.g., outsourced labor, data processing, or manufacturing), risks can arise in any contractual relationship, big or small. These risks can also extend to the suppliers or service providers used by the organization's vendors, known as subservice or fourth parties.

To assess the organization's third-party processes, internal auditors should first determine whether the organization has a structured third-party risk management program as part of its broader enterprise risk management framework. If so, internal auditors can then assess this program to identify the policies, processes, and tools in place for managing third-party risks.

Third-party risk management typically involves three key components:

1. A dedicated framework designed specifically for managing third-party risks
2. A risk appetite statement, which may be organization-wide, specific to a business unit, or tailored for individual third parties
3. A governance structure for overseeing third-party risk management

© Becker Professional Education Corporation. All rights reserved.

6.1.1 Third-Party Risk Management Framework

The purpose of a third-party risk management framework is to ensure that risks associated with third parties are effectively managed and monitored in line with the organization's risk appetite and governance standards. Effective frameworks often share key characteristics such as:

- **Comprehensive Policies and Procedures:** These align with the organization's risk appetite, stakeholder expectations, and industry standards, providing a solid foundation for risk management activities.
- **Robust Governance Structures:** Effective oversight supports the implementation and enforcement of policies and procedures.
- **A Structured Support System,** including:
  - Clearly assigned roles and responsibilities for each of the Three Lines Model and governing bodies.
  - A detailed third-party inventory (vendor master file), risk rating criteria, and a structured risk assessment process.
  - Defined expectations for third-party risk management controls.
  - Reporting requirements for third-party risk exposures, including board-level expectations.
  - A regular, risk-based review process tailored to the nature of the third-party relationships.
  - Processes for classifying, escalating, and tracking issues identified during third-party monitoring activities.

6.1.2 Risk Appetite

To assess whether a third-party relationship aligns with the organization's risk appetite, consider this question: Does the risk exposure from outsourcing or co-sourcing this service, product, raw material, or component fall within the organization's defined risk appetite?

When an organization decides to engage a third party as part of its strategy, management should clearly outline the minimum standards the third party must meet in governance, risk management, and internal control to ensure alignment with the organization's risk appetite.

6.1.3 Third-Party Risk Management Governance

- **Basic Governance Structure**

  In a basic governance structure, managers act as relationship owners, identifying the need for third-party products and services and carrying out due diligence. However, this can lead to conflicts of interest if managers favor certain third parties. Close supervision by oversight functions, senior management, or the board is recommended to mitigate this risk. Another challenge with this model is inconsistent due diligence and review of third parties from management. To address this, organizations may assign one person or team to manage third-party records, including contracts, service level agreements (SLAs), and related documents, ensuring consistent oversight throughout the contract's life cycle.

© Becker Professional Education Corporation. All rights reserved.

- **Defined Governance Structure**

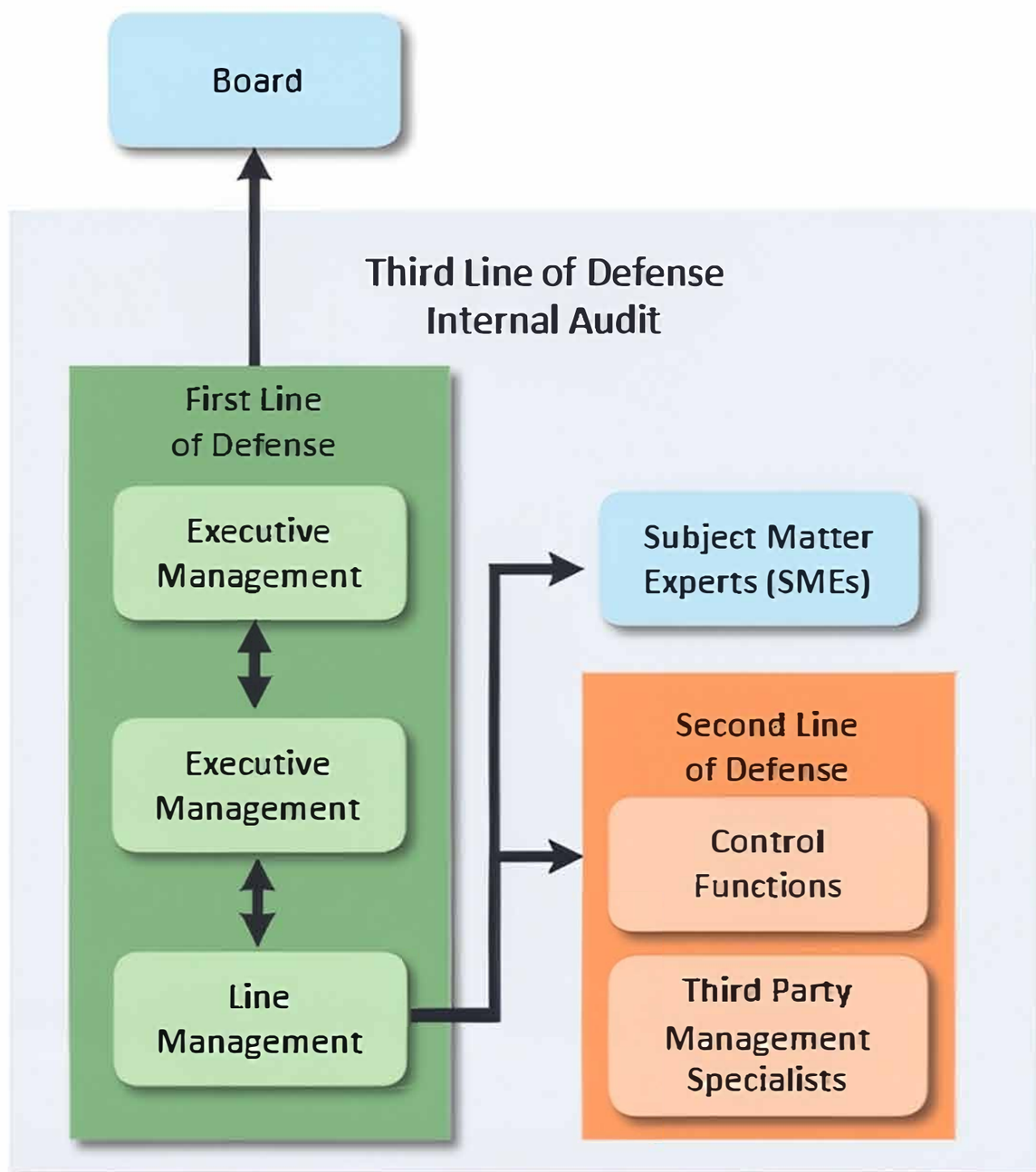
  In organizations with more defined third-party risk management governance processes, personnel assuming a formal Second Line role will support managers in serving as relationship owners. Personnel serving Second Line roles should have the necessary qualifications to carry out their responsibilities, which vary depending on the third party and its relationship with the organization. They may play two key roles:

  1. **Documentation Ownership:** Working with the organization, they may manage third-party documentation such as due diligence records, contracts, SLAs, and insurance certificates.
  2. **Contracting Process Ownership:** In partnership with the organization or as part of the control function, they may oversee the entire contracting process.

- **Standardized Governance Structure**

  In highly regulated industries and complex global organizations, a standardized governance structure is strongly recommended. Third-party specialists, such as procurement or vendor managers, often play a key role in the First or Second Line, depending on the organization's setup. These specialists may handle hundreds of vendor relationships and contracts. Centralizing third-party sourcing, evaluation, and management can improve efficiency, but managers in the First Line roles remain responsible for the third-party risk exposure. In an organization with such a governance structure, internal auditors would assess the work of both the First and the Second Lines.

Third-Party Risk Management Governance—Standardized



Source: The IIA's *Global Practice Guide: Auditing Third-party Risk Management* ©2024, The Institute of Internal Auditors, Inc. Licensed for use.

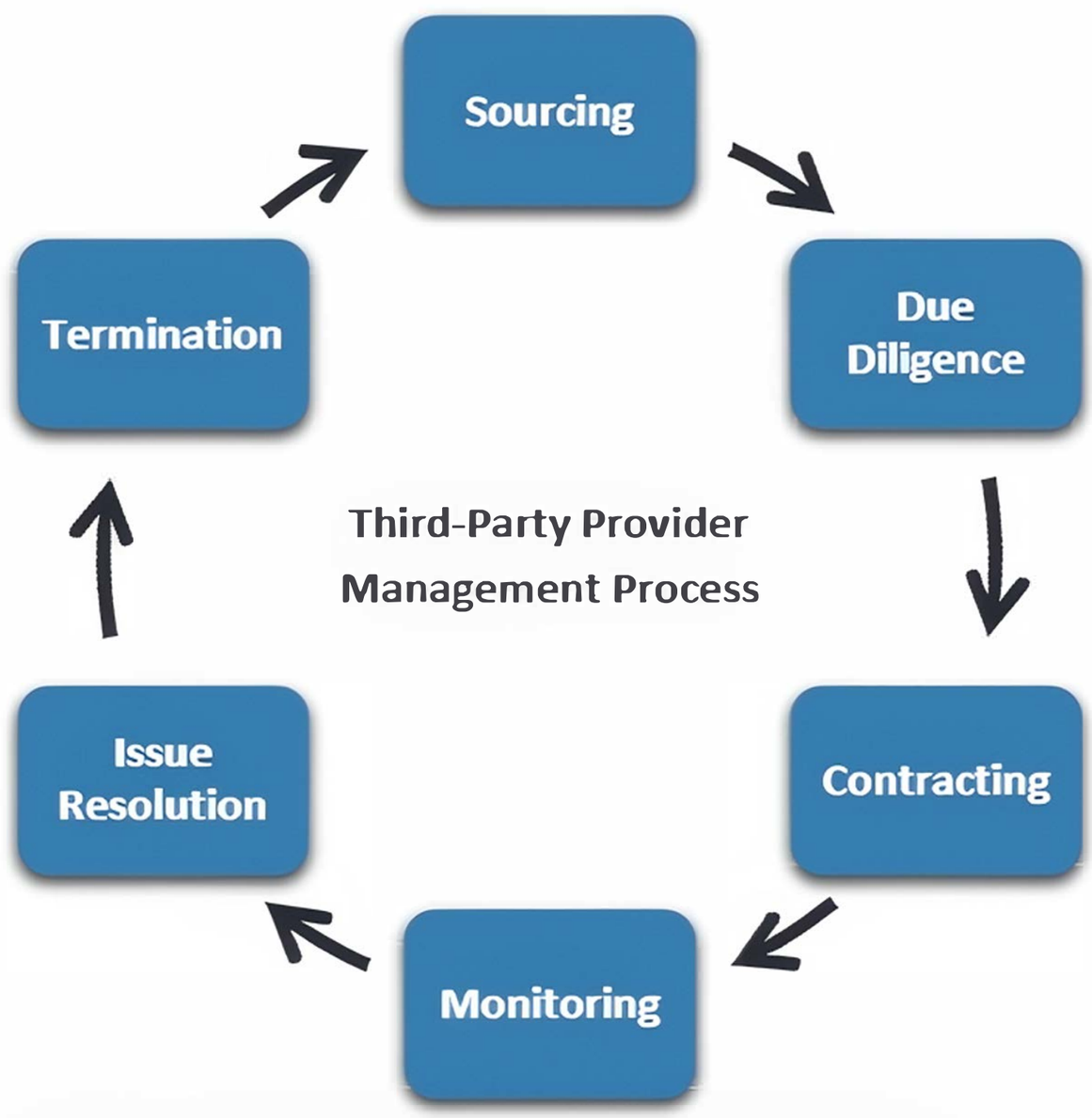
© Becker Professional Education Corporation. All rights reserved.

Pass Key

As the owners of organizational risk, management must continuously identify, assess, manage, and monitor the risks related to each third-party relationship.

6.2 Third-Party Provider Management Processes

When evaluating the overall third-party risk management program or one of its process steps, internal auditors should gain an appropriate level of understanding of the third-party provider management process. Key elements of such a management process include:



Source: The IIA's *Global Practice Guide: Auditing Third-party Risk Management* ©2024, The Institute of Internal Auditors, Inc. Licensed for use.

- **Sourcing:** Management evaluates the business context, strategic objectives, and core competencies of the area to be outsourced. For contracts exceeding a certain monetary value or risk level, a request for proposal (RFP) or invitation to tender (ITT) is issued.
- **Due Diligence:** Management narrows potential candidates by evaluating them against key criteria (e.g., statement of work), conducting risk assessments with input from experts, performing background and performance checks, assessing ethics, and fostering open communication.
- **Contracting:** Contracts outline the organization's risk appetite, minimum internal control standards, and expected service levels for the third party.

© Becker Professional Education Corporation. All rights reserved.

- **Monitoring:** Knowledgeable individuals manage third-party relationships. Decentralized management may apply if a business manager owns the relationship. Key performance indicators (KPIs), risk analyses, attestations, compliance, and relationship status are regularly reviewed.
- **Issue Resolution:** The third-party relationship owner monitors and addresses risks or issues that exceed the organization's risk appetite.
- **Termination:** Contracts include termination conditions, covering aspects like equipment and technology retrieval, separation costs, and other closure requirements.

6.3 Third-Party Process Risks

Some common risks associated with third-party processes include:

- Incompetence or fraud leads to accepting unfavorable bids
- Loopholes arise from poorly worded contracts
- Ineffective contract terms result in liabilities that hurt profitability
- Language or cultural differences cause miscommunication
- Noncompliance or default by the third party is costly to resolve
- Missing auto-renewal deadlines in termination clauses can lead to significant extra costs

6.4 Controls Related to Third-Party Processes

For outsourcing or co-sourcing a business process or functional area, controls may include the following:

- Clearly defined statements of work in the request for proposal (RFP)/invitation to tender (ITT), specifying the scope and its limitations
- Involvement of process owners and stakeholders, such as budget analysts, in creating the RFP/ITT
- Evaluation of bids based on both value and service provider competency
- Justification for sole-source contracts (if applicable) and verification that the chosen provider can deliver the full range of services
- A thorough due diligence process for provider selection, including reference checks
- Assessment of future workforce needs by the process owner to ensure the provider can scale services to meet future demand
- Negotiation of contracts with clear incentives, penalties, and detailed service level agreements (SLAs)
- Inclusion of appropriate clauses in contracts, such as definitions of nonperformance, corrective measures, and termination procedures
- Maintenance of a vendor master file to track performance, document sustainability or ethics agreements, note preferred status, and apply negotiated discounts

© Becker Professional Education Corporation. All rights reserved.

7 Supply Chain Management

7.1 Overview

A supply chain, also known as a logistics network, is the interconnected system responsible for bringing products and services to consumers. It starts with raw materials and ends with the final customer, involving a carefully coordinated flow of information, physical goods, and money. A supply chain can be viewed as a series of interconnected processes or business cycles that transform raw materials into finished products or services for distribution to customers. Different functional areas within various organizations work together to execute these processes.

The most basic supply chain includes the supplier, the producer, and the customer. Connecting these entities are four key flows:

1. **Physical Flow:** The movement of materials and services from suppliers through intermediate entities.
2. **Financial Flow:** The transfer of money from customers back to suppliers.
3. **Information Flow:** The constant exchange of information between all parties.
4. **Reverse Flow:** The return of products for repair, recycling, or disposal.

7.2 Supply Chain Management Processes

Supply chain management processes are used to efficiently design, plan, execute, monitor, and integrate every link in the supply chain. Effective supply chain management ensures that goods and services are produced and distributed in the right quantities in the right place and at the right time in order to minimize system-wide costs while satisfying all the various customers.

The main objectives of supply chain management include:

- Generate value for customers and other key stakeholders through building a competitive infrastructure, leveraging worldwide logistics, matching supply with demand, and tracking performance effectively.
- Effectively manage supply chain risks, such as risks associated with the availability and quality of suppliers and their products or services, as well as risks related to the distribution of products or services to customers.

The most important processes in supply chain management are customer relationship management (CRM) and supplier relationship management (SRM).

7.2.1 Customer Relationship Management

Customer relationship management (CRM) is both a customer-centric philosophy and a strategic approach to fostering strong customer relationships. It includes a set of methodologies and tools designed to prioritize customer needs and enhance interactions.

© Becker Professional Education Corporation. All rights reserved.

The CRM process involves finding customers, understanding their potential needs, and building and maintaining a loyal customer base. It involves a collaborative effort across different functions (e.g., product design, operations, and finance) who work closely with customers to:

- Identify product and service needs, and create product service agreements (PSAs) that outline the terms of the relationship.
- Optimize order and deliver processes and eliminate unpredicted variation in demand.

CRM systems, installed or cloud-based, play a crucial role in supporting this philosophy by enabling well-informed communication and interactions with customers.

The primary purpose of CRM systems is to consolidate and organize customer information for easy access, ensuring that all interactions—from sales representatives to customer service teams—are informed and consistent. This system provides:

- Records of the latest customer communications.
- Updates on order or complaint statuses.
- Insights into customer preferences or special requirements.

Additionally, CRM systems support various functions, including tracking prospective customers through the sales pipeline, prompting salesperson follow-ups by territory, managing marketing outreach (e.g., emails), performing lead scoring and customer segmentation, handling quotes and responses to proposals, and automatically transitioning converted leads into customer accounts.

7.2.2 Supplier Relationship Management

While CRM emphasizes building loyalty with key customers, supplier relationship management (SRM) focuses on developing long-term relationships with key suppliers. Building supplier relationships may vary depending on the industry or organization. Determining the organization's supply needs is also a cross-functional effort that typically involves marketing, research and development, production, logistics, and finance.

SRM is a critical risk management activity. This is because a supplier's actions and ethical standards, even if they operate independently, can directly influence an organization's reputation and other enterprise risks. Therefore, key aspects of SRM include identifying dependable and ethical suppliers and confirming that their operations align with robust governance, risk management, and control frameworks.

7.3 Risks and Controls in Supply Chain Management

7.3.1 Key Risks in Supply Chain

With organizations' increasing reliance on outsourcing, internal audit teams should carefully assess the quality and environmental risks associated with an organization's supply chain. International standards usually require that organizations oversee their suppliers to ensure that products meet customer expectations. Furthermore, the lines between organizations are becoming less distinct due to advancements in technology, a reality with significant implications for internal auditors. There is also a shift from traditional contract-based supply chains toward more fluid, free-market approaches.

© Becker Professional Education Corporation. All rights reserved.

These evolving dynamics introduce new supply chain risks, including:

- **Overreliance on a Single Supplier:** Organizations may become vulnerable if they depend too heavily on one source for a critical component.
- **Challenges With International Suppliers:** Offshoring can present obstacles related to language barriers, management practices, and transportation logistics.
- **Inadequate Management Systems:** Supply chain management systems that fail to address customer and supplier relationship concerns can create inefficiencies and risks.

7.3.2 Addressing Risks in Supply Chain

- **Supplier Diversification:** Organizations should adopt a strategy to diversify suppliers, especially for critical goods and services. This may include regularly assessing supplier performance and financial stability, identifying alternative suppliers in the case of disruptions in primary suppliers, and maintaining a sufficient inventory buffer for critical goods.
- **Managing International Suppliers:** To effectively manage international suppliers, organizations should establish clear communication protocols taking into consideration differences in time zone and language. Additionally, contract management procedures should be in place for quality control and dispute resolution.
- **Adequate Management Systems:** Organizations should implement a comprehensive supply chain management system to ensure that all aspects of the supply chain are integrated. An efficient management system should allow effective communication and collaboration among various parties within the supply chain. Management should conduct ongoing assessments and updates of the system to ensure alignment with organizational needs and technological advancements. Furthermore, regular training of employees on the use and maintenance of the system is also necessary to ensure system efficiency.

8 Software Systems

8.1 Enterprise Resource Planning Systems

Enterprise resource planning (ERP) systems are cross-functional systems that support different organizational functions and facilitate integration of information across departments such as accounting, customer management, finance, human resources, inventory management, manufacturing, marketing, and vendor management.

An ERP solution facilitates real-time communication between systems and typically operates under a centralized database and user interface. This interface may offer multiple modules that function independently or as an integrated system that allows data to be shared across different departments or divisions of an organization.

© Becker Professional Education Corporation. All rights reserved.

Advantages of using ERP systems include:

- A centralized, integrated database, which eliminates duplicate records and ensures a consistent, up-to-date single source of "truth"
- Fully integrated and automated interactions between business processes, enabling robust and configured internal controls

ERP systems can be very expensive and complicated. Upgrading or customizing ERP systems can be even more costly. Given the high stakes, organizations should prioritize optimizing these systems for efficiency and effectiveness in order to achieve substantial cost savings.

8.2 Governance, Risk, and Compliance Systems

Governance, risk, and compliance (GRC) systems enhance organizational frameworks and programs by automating many documentation and reporting tasks related to risk management and compliance. GRC systems are designed for a range of users, including audit committees, executives, internal auditors, and risk and compliance managers.

- **Internal auditors** can leverage a GRC system to:
  - Manage workpapers efficiently.
  - Schedule engagements and related tasks.
  - Handle reporting and time management requirements.
  - Access and review organizational GRC documentation for assurance and advisory engagements.
  - Conduct data analytics using tools for credit risk or market risk assessment.
- **Risk and compliance managers** use GRC systems to create, review, distribute, and update policies, aligning them with organizational objectives and linking them to associated risks and controls.
- **Compliance professionals** can document, visualize, and report on control objectives, controls, related risks, and control self-assessments.
- **Risk management professionals** benefit from consolidated risk analysis, enabling streamlined communication and reporting.

While cloud-based GRC systems are available, installed software remains more widely used, largely due to concerns around security and privacy.

© Becker Professional Education Corporation. All rights reserved.

8.3 Key Risks and Controls for Software Systems

Software systems usually include operating systems, network and communication software systems, firewalls, antivirus systems, and database management systems. Given the complexity of software systems, effective controls need to be in place to mitigate critical risks associated with these systems.

Key risks and controls related to software systems include:

Key Risks	Key Controls to Mitigate Risks
Unauthorized access	• Appropriately controlled and allocated access rights based on organizational policies • Using encryption where confidentiality is required
System vulnerability	• Intrusion and vulnerability assessment, prevention, detection, and ongoing monitoring • Regular intrusion testing
Malware attacks	• Malware protection and monitoring (e.g., continuous monitoring, prevention, and quarantining of threats)
Inadequate performance management	• Perform regular performance management procedures to monitor system operations and resolve software system issues • Implement change management processes to ensure controlled updates to software, systems, networks, and data
Fraud risks	• Segregation of duties enforced through systems software and other configuration controls

© Becker Professional Education Corporation. All rights reserved.

NOTES

© Becker Professional Education Corporation. All rights reserved.

MODULE

7 Appropriate Engagement Approach

Part 2
Unit 1

This module covers the following topics from the *CIA examination syllabus*:

CIA Syllabus—Section A: Engagement Planning
4. Determine the appropriate approach for an engagement *May include but is not limited to:* a. Evaluate various approaches such as agile, traditional, integrated, and remote auditing to determine the most suitable approach b. Describe project management concepts as they relate to planning and conducting an engagement

1 Considerations for Determining the Engagement Approach

The internal audit function should consider what is the most suitable approach for an engagement based on several factors, including:

- Resources available (financial, human, and technological) to perform the engagement work
- Timeline of the engagement (long-term versus short-term)
- Anticipated level of changes to the scope, timing, or resources for the engagement
- Level of dependencies of the tasks to be performed
- Interdependencies between processes and whether processes span multiple departments
- Location of personnel working in the activity under review (on-site versus remote)

Additionally, the available technology applications are another consideration in determining whether it is suitable to perform the engagement remotely.

The CAE should determine the most appropriate approach based on a careful analysis of the organization, specific risk considerations, the activity to be reviewed, and overall resource availability.

Project management is also critical in managing the efficiency of the engagement and helping ensure the engagement objectives are achieved. Tracking and monitoring the various resources and activities can help identify potential risks and issues early on so that they may be addressed appropriately and do not jeopardize the success of the engagement.

© Becker Professional Education Corporation. All rights reserved.

2 Traditional Auditing

2.1 Overview of Traditional Auditing

Traditional auditing uses what is referred to in project management as a waterfall approach. This approach involves a structure with a series of phases (engagement planning, fieldwork, review, and reporting) that are performed in sequence with no overlap or consecutive activities. The approach is often described as rigid, and it usually takes longer to complete the engagement process.

The tradtional approach can also be less adaptable to change or lack timely and frequent interaction with stakeholders, which are features that are becoming more essential for the success of internal audit services.

A traditional auditing approach would be suitable for engagements:

- With a longer timeline and fewer resources to allow for the team to perform the work in a sequential order over a long period of time.
- With no or few anticipated changes to scope, time, and resources that would require flexibility and the ability to easily make changes to the project/engagement plan.
- When there are a lot of dependencies among the tasks to be performed that may hinder the ability to perform tasks simultaneously or with overlap.

An example of when a traditional auditing approach may be suitable is when a risk assessment concludes that a high-risk area needs immediate attention. In such a situation, a focused, traditional audit may be effective. For smaller organizations with limited staff, a traditional approach might be necessary to minimize disruption to daily operations.

Pass Key

A traditional auditing approach uses what is referred to as a waterfall method approach, where activities are completed in sequential order. Therefore, this approach may be suitable:

- When there is a long timeline for the engagement.
- When there are limited resources to perform the tasks.
- When there is a low risk of changes to the plan during the engagement.

© Becker Professional Education Corporation. All rights reserved.

3 Agile Auditing

3.1 Overview of Agile Auditing

Originating from the agile methodology initially used in software development, agile auditing is an innovative approach to internal auditing characterized by its speed, flexibility, collaboration, and iterative progress throughout the engagement process.

Agile auditing is particularly useful in a changing and dynamic business environment that requires internal auditors to prioritize adaptability and responsiveness to ensure the relevance and efficiency of the internal audit function in supporting the organization. A primary focus of the agile auditing approach is efficiency.

There is no one methodology for agile auditing because it is customized to the organization. Agile auditing typically breaks down an engagement into short, focused sprints that involve simultaneous planning, fieldwork, review, and reporting. Each sprint builds upon the previous one, creating a continuous cycle that incorporates feedback and adapts to new information or changes.

Such an iterative approach allows internal auditors to assess, monitor, and promptly respond to emerging risks and issues on an ongoing basis. It helps internal auditors prioritize activities based on their importance, urgency, and the team's availability to do the work. Agile auditing can be effective in both assurance and advisory engagements.

Agile auditing would be a suitable approach for engagements:

- With a shorter timeline.
- With anticipated changes in scope and resources.
- When there are not a lot of dependencies, allowing for tasks to be performed simultaneously or with overlap.

3.2 Benefits of Adopting Agile Auditing

- **Increased Efficiency:** One of the primary benefits of agile auditing is increased efficiency and speed in the engagement process. It facilitates streamlining risk assessment processes, resulting in quicker decision making and timely resolution of issues. It also allows for faster reporting turnaround time. For example, sometimes the report delivery time can be reduced from over a month to within a week after adopting the agile approach.
- **Better Collaboration and Transparency:** By engaging stakeholders throughout the engagement process, agile auditing promotes greater transparency and leads to more accurate and comprehensive assessments of risks and controls. Such collaboration enhances stakeholder support and ensures alignment between the internal audit team and the stakeholders' expectations and needs.
- **Greater Adaptability and Focus:** Agile auditing provides the flexibility for internal auditors to respond to changes and evolving business conditions. It also optimizes the use of internal audit resources by prioritizing high-risk areas and ensuring the timely delivery of valuable insights.

© Becker Professional Education Corporation. All rights reserved.

3.3 Implementing Agile Auditing

Applying Scrum techniques is considered an effective means of implementing agile auditing. Scrum is a project management framework that prioritizes teamwork, accountability, and iterative progress toward a well-defined goal.

Under the Scrum framework, the engagement process is broken down into short, focused sprints. Some sprints can last one to two weeks; others can take a month or so. Each sprint involves completing a set of tasks, usually referred to as "user stories," that contribute to the overall engagement objectives. At the end of each sprint, the internal audit team delivers a working product to the stakeholders and gathers feedback for continuous improvement.

The life cycle of the sprint consists of several key steps that can be applied to agile auditing:

- **Step 1: Sprint planning.** The internal audit team conducts a planning session before each sprint to determine the scope of work. The session involves discussions on key risks and controls identification, testing procedure determination, alignment of goals, and what defines the completion of tasks in that sprint. Both internal auditors and management of activities under review should actively participate in the session to ensure clarity and a thorough understanding of expectations, as well as create buy-in among the internal audit team.
- **Step 2: Frequent check-ins.** Throughout the sprint process, internal auditors conduct frequent check-ins (e.g., daily 15-minute meetings) within the internal audit team. During these check-in meetings, the team can share their progress, accomplishments, plans for the remaining process, and any challenges they are facing. Frequent check-ins foster collaboration amongst team members, promote transparency, and allow prompt problem identification, ensuring the achievement of the sprint goals.
- **Step 3: Sprint review and reporting.** At the end of the sprint, internal auditors meet with management and other key stakeholders to review the output of the sprint and decide on the next steps. This collaborative review allows the team and stakeholders to assess progress, adjust priorities, and plan for the upcoming sprint. It also enhances continuous feedback and alignment between the internal audit team and stakeholders.
- **Step 4: Retrospective reviews.** As the final stage in the sprint life cycle, a retrospective review is performed at the conclusion of each sprint to identify areas for improvement. The internal audit team, management, and other key stakeholders can participate in the review to discuss what went well, what could be improved, and how to enhance quality and effectiveness in future sprints.

By following the Scrum framework, agile auditing enables the internal audit function to respond faster to changes, deliver continuous value to stakeholders, and stay relevant in a dynamic business environment.

© Becker Professional Education Corporation. All rights reserved.

3.4 Addressing Challenges in Adopting Agile Auditing

While highly beneficial if implemented successfully, agile auditing adoption also involves multifaceted challenges regarding shifts in mindset and culture, team formation, training, and resources.

- **Shifts in Mindset and Culture:** Agile auditing requires a fundamental shift in mindset on how engagements are conducted and a change in culture within the internal audit function. However, resistance to change within the organization can arise, especially from key stakeholders and internal audit team members who are accustomed to traditional auditing methods. Addressing these concerns requires clear communication and demonstration of benefits, as well as comprehensive training and strong support throughout the transition. To successfully implement agile auditing, internal auditors should also embrace adaptability and collaboration. The culture shift requires strong support from the top and a commitment to continuous improvement. Therefore, it may be easier to suggest and implement an agile approach in an environment where there is little resistance to a change in engagement approach.
- **Team Formation:** To ensure effective agile auditing, the CAE should assemble a team with individuals who possess the diverse knowledge and skill sets necessary to perform the tasks. Roles and responsibilities within the internal audit team should also be clearly defined to ensure accountability and focus. It may be difficult to implement an agile engagement approach where internal audit team members do not have and are not able to obtain the appropriate knowledge or skills to be able to perform all the activities needed for the engagement.
- **Training and Resources:** Equipping internal audit teams with the necessary knowledge and tools is crucial for successful agile auditing implementation. Organizations should invest in training and education of internal auditors on agile methodologies and best practices. Additionally, providing sufficient access to tools and resources (e.g., project management software, collaboration platforms) can enhance efficiency and facilitate communication within the team. Therefore, it may be a challenge to implement an agile approach if there is no ability (lack of budget, time, or resources) to provide the appropriate training and tools to perform the engagement.

Illustration 1 Team Formation in a Traditional Approach vs. Agile Approach

Traditional approach:

The internal audit function at a bank is adopting an agile audit approach in the coming year. In prior periods, team members were assigned to individual engagements based on scheduled start and end times, and following the completion of an engagement, team members went on to join other teams. The overall focus was on the completion of the engagement.

Agile approach:

In the coming year, internal audit teams were formed for the entire audit cycle and were assigned a series of engagements for the year. The internal audit teams were responsible for completing the series of engagements, with increased flexibility regarding how and when each individual engagement was completed. While the engagements will all be completed during the year, the real focus is on the success of the team through coaching and growth and engagement successes.

© Becker Professional Education Corporation. All rights reserved.

Pass Key

Agile auditing would be a suitable approach in an engagement with a shorter timeline and for a changing and dynamic business environment that may require flexibility to change the engagement plan to adapt to changes in the scope, cost, or resources impacting the engagement.

Also, the internal audit function needs a sufficient team with the appropriate knowledge and skills to perform the engagement tasks.

4 Integrated Auditing

4.1 Overview of Integrated Auditing

An integrated approach to internal auditing is a systematic, innovative, and flexible approach that aims to create value for the organization by integrating various aspects of internal auditing. It may involve conducting integrated audits, which include combining different audit disciplines, such as financial, operational, and IT audits, into a single audit.

More importantly, an integrated approach focuses broadly on integration considerations or options over various stages of the internal audit process (engagement objectives and scope, audit techniques and execution, resource management, and reporting) to maximize value and meet the needs of key stakeholders.

Integrated approaches to internal auditing facilitate more agile development of objectives, scope, resource options, knowledge transfer, audit techniques, and issue perspectives and solutions, leading to more holistic and insightful internal audit services.

Traditional auditing typically focuses on separate audits of specific areas or disciplines, such as financial or operational audits. Integrated auditing differs from traditional auditing in terms of its scope, coverage, depth, and overall complexity. Integrated auditing takes a more holistic approach, combining different disciplines and considering a broader range of integration options, such as risks and controls, governance processes, strategic alignment, and sustainability considerations. This approach emphasizes a more comprehensive assessment of the organization's overall risk profile and can lead to more effective and efficient audits.

It may be most suitable to use an integrated audit approach in larger and more complex organizations, including public companies, especially when there are interdependencies between processes and processes span multiple departments. This allows multiple aspects to be considered simultaneously to allow for a more holistic understanding achieved in a more efficient manner. Examples of such integrated audit engagements include:

- Financial and operational audits
- IT and business process audits
- Compliance and risk management audits

© Becker Professional Education Corporation. All rights reserved.

An integrated audit approach may also be suitable in organizations with a smaller internal audit function and limited staff and resources. There are several benefits to using an integrated approach in such situations, including increasing efficiencies and effectiveness of risk coverage, enhancing the presence of the internal audit function in the organization, and expanding the knowledge and skills of the internal audit team members by having them work on broader and more complex audit engagements. However, resource or budget constraints could make a large-scale integrated audit engagement impractical.

4.2 Benefits and Challenges of Integrated Auditing

As noted in The IIA's *Global Practice Guide: Integrated Approaches to Internal Auditing,* there are numerous benefits to an integrated auditing approach, including:

- **Increased efficiency and operational improvements**—streamlining processes and leveraging resources across different areas, resulting in greater efficiency and operational effectiveness.
- **Holistic risk assessment**—promoting a more comprehensive understanding of risks to ensure alignment with business objectives.
- **Strategic alignment**—providing greater assurance that organizational strategies are well-aligned.
- **Strategic solutions**—fostering the development of innovative, cost-effective, and sustainable solutions to address organizational issues and mitigate risks.
- **Business focus and value creation**—driving a stronger focus on business needs and maximizing value creation for the organization.
- **Enhanced organizational understanding**—enhancing the internal audit function's understanding of the organization, creating more opportunities to develop diverse skills and knowledge across the team.
- **Increased credibility and relevance**—improving the internal audit function's credibility and relevance within the organization by providing more insightful and impactful internal audit services.
- **Reduced audit fatigue**—minimizing disruptions to the organization by consolidating audit efforts and streamlining interactions with stakeholders.
- **Data-driven insights**—leverages data analytics and tools to generate meaningful insights, enabling more effective decision making.

However, integrated approaches also present challenges, such as increased complexity in scope and coverage, the need for specialized skills and knowledge, and potential difficulties in coordinating and communicating across different disciplines and areas.

Pass Key

The internal audit function typically considers integration options in audit processes when developing either the internal audit plan or the engagement plan.

© Becker Professional Education Corporation. All rights reserved.

5 Remote Auditing

5.1 Remote Auditing

Remote auditing differs from traditional auditing primarily in the location where the engagement activities are conducted. While traditional auditing requires internal auditors to physically be present on-site to perform engagement procedures such as interviews, document reviews, and process evaluations, remote auditing can be performed from a distance by leveraging technology tools.

The location shift brings both benefits and challenges for the internal audit function. Remote auditing clearly provides benefits through reduced travel time and costs, an expanded pool of available team members, potentially broader coverage due to time savings, and reduced burden on facilities of the activities under review.

Nevertheless, remote auditing also presents challenges, including limited access to certain types of evidence (e.g., inventory auditing), difficulties in building relationships remotely with key stakeholders, and the potential for increased fraud risk due to lack of in-person contact.

Regardless of these challenges, remote auditing becomes more prevalent when travel is restricted and alternative approaches are needed to perform internal audit engagements. With the development of technology that enables internal auditors to adapt their methodologies, remote auditing will potentially remain a significant alternative to traditional auditing.

As mentioned in the Internal Audit Foundation and AuditBoard Report: *The Remote Auditor: Challenges, Opportunities, and New Ways of Working*, published in 2021, it may be suitable to use a remote auditing approach in certain industries such as business services, health care and social assistance, finance, and insurance where personnel may be more likely to be working from home. Other industries where personnel tend to be in-person on-site, such as educational services, public administration, and manufacturing, may be less suitable for remote auditing.

Additionally, a remote auditing approach may be suitable when the internal audit function has the appropriate technology solutions to be able to work collaboratively and mitigate risk management concerns. Technology solutions are needed to perform various tasks remotely, such as interviews, walk-throughs, and physical observations. Audit software is needed to facilitate audit documentation and reviews as well as other elements of internal audit processes.

© Becker Professional Education Corporation. All rights reserved.

Pass Key

When choosing between remote auditing and traditional, on-site auditing, the following factors should be taken into consideration:

- Cost savings
- Internal audit resources, including human and technological resources
- Types of procedures that need to be performed
- Types of evidence that can be obtained
- Security of communications
- Timing
- Potential risk factors (e.g., fraud risk)

5.2 Considerations for Performing Remote Auditing

Effective and efficient remote auditing requires internal auditors to consider the following:

- **Communication:** Effective communication is critical for the success of remote auditing. Maintaining frequent communication, both formal and informal, is essential for keeping all parties informed and engaged. Besides formal communications, internal auditors should consider scheduling additional online meetings for activities such as engagement planning, mid-week status updates, end-of-the-week wrap-ups to ensure everyone is aligned, discussions on issues identified, and reviews of report drafts.
- **Conducting Interviews:** When conducting remote interviews with the management of the activity under review, internal auditors should be mindful of the duration of the interviews. For example, shorter interviews, such as 30–60 minutes per session, are considered ideal because multiple sessions may be needed to collect all relevant information.
- **Document Reviews:** Reviewing documents remotely can be more time-consuming if the documents need to be prepared and uploaded to a file-sharing platform. To streamline the process, internal auditors can consider requesting temporary direct access to digital documents for the duration of the engagement.
- **Skills Needed:** The shift to remote auditing has highlighted the significance of certain skills internal auditors may need, including technology proficiency, adaptability, interpersonal skills, data analytics, and critical thinking skills. For instance, internal auditors should be comfortable navigating various digital tools and technologies for communication, data analysis, and evidence collection. Despite reduced in-person interaction during remote auditing, internal auditors still need to maintain strong communication skills and build stakeholder relationships remotely. Furthermore, successful remote auditing requires that internal auditors are proficient at analyzing data, identifying trends, drawing meaningful conclusions, and generating actionable insights in a remote environment.

© Becker Professional Education Corporation. All rights reserved.

6 Comparison of Engagement Approaches

Pass Key

The following table helps summarize some of the considerations when determining the most suitable engagement approach.

	Approach			
	Traditional (Waterfall)	**Agile**	**Integrated**	**Remote**
Characteristics	"Waterfall" approach where activities are performed in sequential order	Iterative approach – each sprint/activity builds upon the previous one, creating a continuous cycle that incorporates feedback and adapts to new information or changes	Systematic, innovative, and flexible approach that involves conducting integrated audits, which include combining different audit disciplines, such as financial, operational, and IT audits, into a single audit Focuses broadly on integration considerations over various stages of the internal auditing process (audit objectives and scope, audit techniques and execution, resource management, and reporting) to maximize value and meet the needs of key stakeholders	Off-site
Engagement duration	Long-term	Short and tight	Constrained	No impact
Internal audit team resources	Limited	Large	Limited	No impact
Technology resources	No impact	No impact	No impact	Critical/required to enable off-site work
Subject to changes	No or limited flexibility	Allows for flexibility	No impact	No impact
Task dependencies	Lots of dependencies	Limited dependencies	Consistent processes across departments	No impact
Organization characteristics	Organizations with a smaller internal audit function	Organizations with a changing and dynamic business environment, with a larger internal audit function or budget for external internal audit service providers	Larger and more complex organizations, including public companies	Organizations in the following industries: Business services, health care and social assistance, finance, and insurance, where personnel may be more likely to be working remotely

© Becker Professional Education Corporation. All rights reserved.

7 Project Management

7.1 Introduction

Project management is essential for internal auditors to plan and conduct engagements because it helps ensure that engagements are completed on time, within budget, and in compliance with project requirements. It involves careful planning, organizing, and controlling resources to meet engagement objectives. Effective project management requires internal auditors to define scope, allocate resources, and manage time and costs to ensure the delivery of high-quality work.

A project typically involves a series of tasks and activities, utilizes resources, and operates within constraints such as time (e.g., project start date, timeline, and target completion date) and budget. Projects aim to fulfill an organization's needs or requirements by achieving specific objectives that guide their path toward a defined goal.

Successful project management includes delivering a project that achieves its objectives by optimizing the allocation and integration of inputs and reaching a desired performance or quality level within a defined time and budget.

Project management techniques may help internal auditors avoid common problems such as:

- **Scope creep**—an increase in the amount of work, resources (financial or human resources), or time on the project (after it has begun) not originally planned for due to poor planning or unanticipated changes in circumstances impacting the project.
- **Gold plating**—performing work that is beyond the scope of the project and project objectives without approval that may also impact the project costs and deadlines.
- **Rework**—reperforming tasks that may have been inappropriately planned for (inappropriate resources or timing allocated to the original tasks resulting in incomplete or inaccurate results).

Scope creep and gold plating can be significantly problematic (negatively impacting project time, cost, and/or quality) when internal or external stakeholders are allowed to add requirements to a project without providing appropriate resources (e.g., money and time) to complete additional work.

Pass Key

Project management involves the planning and monitoring of the following elements related to a project or engagement:

- Timeline
- Cost
- Resources (human and technological)
- Scope (tasks)
- Quality

© Becker Professional Education Corporation. All rights reserved.

7.2 Project Life Cycle

A project usually progresses through different stages during its life cycle. The project life cycle consists of a series of phases that a project goes through from its initiation to its closure. It provides a structured approach to managing projects. While their names and specifics may vary across industries, these stages typically include:

- **Initiation:** The project's goals, objectives, nature, and scope are defined. Obtaining senior management support and understanding stakeholder expectations are crucial at this stage. A project charter is developed to formalize the project and authorize resources and funding. The project manager and project team are then determined. Members of a project team often play the following roles:
  - Project stakeholder—key stakeholders include the project manager, the customer or end-user (e.g., the board for internal audit projects), and the project team. These individuals are either actively involved in the project or affected by the project's outcome.
  - Project sponsor—the person or group who initiates the project, secures resources, and advocates for its success.
  - Project manager—the project leader responsible for planning, executing, and completing the project within the defined constraints.
  - Project team—the group of individuals with diverse skills assembled to carry out the project's tasks.
- **Planning and Design:** Schedules/timelines, budgets, and resource allocation are determined at this stage, laying the groundwork for successful execution. Examples of project tasks to be performed in this phase may include:
  - Defining work requirements, including the quantity and quality of work
  - Establishing the budget and determining the resources needed
  - Developing the project timeline, including milestones
  - Defining project deliverables and documentation, as well as performance measurements
  - Developing a project management plan that includes all the components (timeline, budget, list of deliverables, etc.) and obtaining formal approval
- **Execution and Production:** The project's work is performed according to the plan. Examples of project tasks to be performed during this stage may include:
  - Launching the project management plan and confirming the availability of adequate and appropriate resources
  - Work is performed and provides status updates
  - Documenting work performed, providing status updates to key stakeholders, and producing deliverables

© Becker Professional Education Corporation. All rights reserved.

- **Monitoring and Control:** The project manager tracks progress, manages resources, and oversees the quality of the work. This stage involves actively keeping the project on track and within budget.
- **Completion and Evaluation (Closure):** The project is finalized, deliverables are distributed, and performance is evaluated. A client's sign-off may be obtained as evidence of the acceptance of deliverables. Performance evaluation usually involves assessing the project's effectiveness at the final stage (e.g., measuring stakeholder satisfaction). Lessons learned are documented to improve future projects.

7.3 Project Management Triangle

The project management triangle (also known as the triple constraint) shows the interdependence of time, cost, and scope in managing any project. All three of the components of the triangle impact the quality of the project. These constraints are interconnected, implying that a change in one inevitably impacts the others.

- **Time**—the amount of time available to complete the project, including the time required for each task and component.
- **Cost**—the budget available to complete the project is determined by factors like labor rates, material rates, equipment (including technology applications), and organizational profitability.
- **Scope**—the project's defined objectives (i.e., what the project is supposed to accomplish) and deliverables (i.e., what the end result is supposed to be) and the tasks to be performed to achieve those.
- **Quality**—the quality is sometimes represented inside the triangle to represent that the quality of the project's outcome is influenced by the timeline, the cost expended on resources, and the tasks performed.

The triangle illustrates the trade-offs inherent in project management. For instance, increasing scope often requires more time and cost input. Similarly, a tight time constraint may require increased costs and a reduced scope, which may compromise project quality.

Skilled project managers use a variety of tools and techniques to balance these constraints and deliver successful projects. When changes threaten the project's feasibility within the constraints, the project manager should communicate with management or a change control board in a timely manner.

© Becker Professional Education Corporation. All rights reserved.

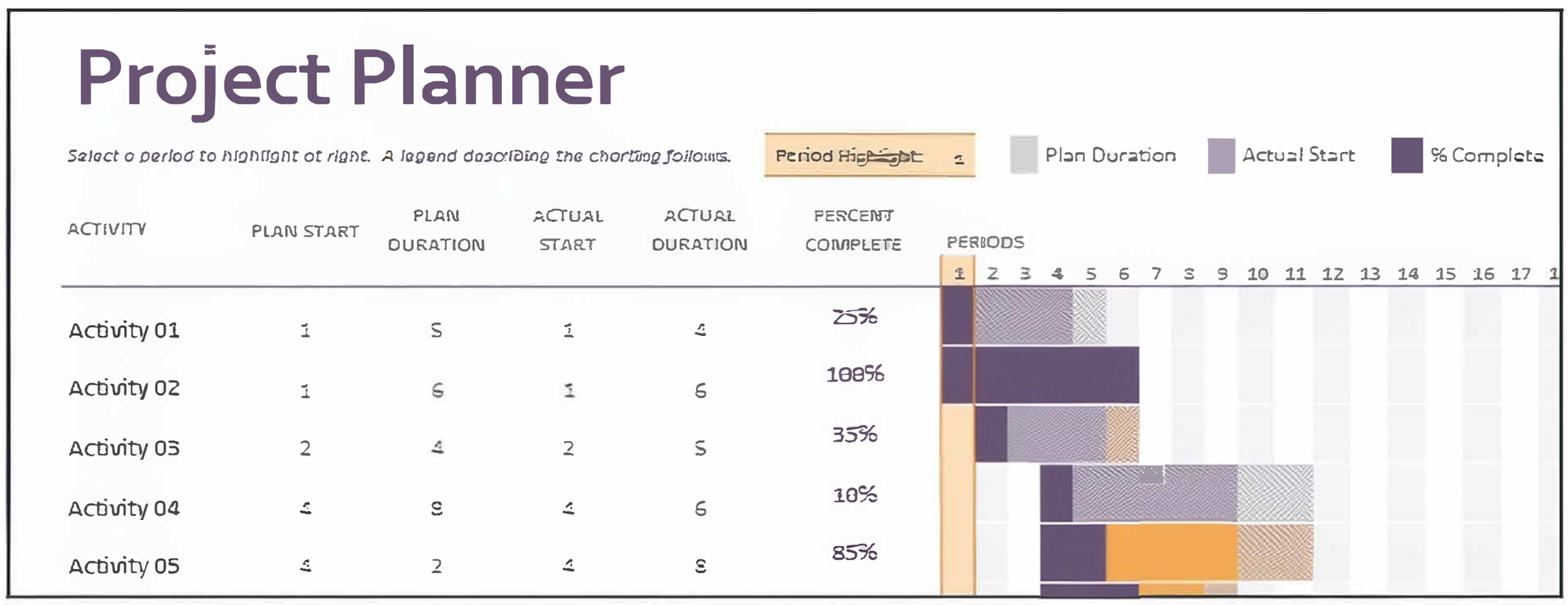
7.4 Project Management Techniques

Various tools and techniques, such as Gantt charts and network analysis, can help with project planning and management.

7.4.1 Gantt Chart

A Gantt chart is a visual tool that helps project managers schedule and track project activities. It displays tasks as horizontal bars, showing their start and end dates, durations, and sequence of activities. This allows for easy visualization of the project timeline and helps identify potential scheduling conflicts or delays.

An example of a Gantt project planner provided by the Microsoft Corporation in Excel illustrates the tracking of activities by time period and duration.



Gantt charts are valuable for planning tasks, scheduling resources, and determining the path—the sequence of tasks that must be completed on time to meet the project deadline. They are particularly useful for internal audit projects, given the engagement process generally follows a predictable sequence.

7.4.2 Network Analysis

Network analysis, often using techniques such as the program evaluation review technique (PERT) and the critical path method (CPM) that are often referred to as PERT/CPM, helps evaluate a project's tasks and their dependencies to find the most efficient path for reaching the project goals. This scheduling tool also helps with tracking resource costs and usage.

The three elements used to develop a network analysis include:

- Tasks
- Time to complete the tasks
- Sequence of tasks, including identifying dependencies

Network analysis allows project managers to coordinate complex projects, optimize the schedule, and identify opportunities for reducing costs by shortening or revising the sequence of tasks. It can be helpful to internal auditors in determining the impact of risks and controls on engagements, particularly in industries with complicated processes.

© Becker Professional Education Corporation. All rights reserved.

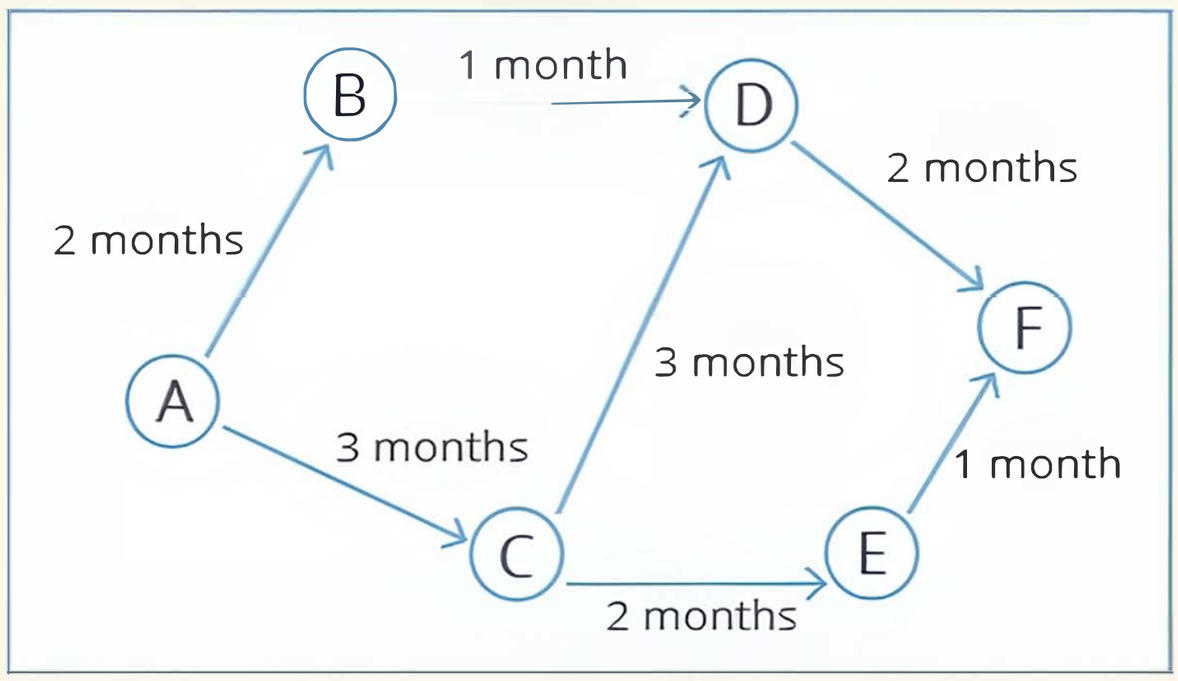
Identifying the critical path is the goal of adopting network analysis.

- Critical path is defined as the sequence of activities without slack time that will collectively take the longest to complete, which indicates the shortest possible total project duration.
- Slack time is the amount of additional time that an activity can be delayed without delaying the overall project.

This means that any delay in the activities on the critical path delays the overall schedule. Tasks that are not on the critical path may have slack and, therefore, could allow delays without affecting the overall schedule until their slack is used up.

Illustration 2 Network Analysis Using PERT/CPM

The following PERT/CPM chart shows the sequence of tasks in an internal audit project. Each circle represents a task, and the arrows show the order of the tasks. The numbers on the arrows represent the number of months it takes to complete each task.



To find the critical path, the internal audit team needs to identify the longest path through the network:

- **Path A-C-D-F:** 3 + 3 + 2 = 8 months
- **Path A-B-D-F:** 2 + 1 + 2 = 5 months
- **Path A-C-E-F:** 3 + 2 + 1 = 6 months

According to the calculation, the longest path from start to end is path A-C-D-F, which is the critical path. Therefore, the time it takes to complete the tasks along path A-C-D-F, 8 months, is the shortest overall time the internal audit project can be completed.

© Becker Professional Education Corporation. All rights reserved.

7.4.3 Project Management Techniques for Addressing Delays and Conflicts

There are several techniques that project managers may use to help in addressing unexpected delays or resource conflicts that may arise during a project/engagement. These include:

- **"Fast Tracking" or Adding Lead Time:** In this method, a task is accelerated to begin before its predecessor task is completed. This causes the tasks to be performed simultaneously, when possible. The risk with this approach is the rework of the successor task based on the work and findings of the predecessor task.
- **Slack Time:** For activities not on the critical path, using slack time allows for the ability to delay the start time of these tasks if needed.
- **"Crashing":** Crashing is referred to as adding resources to the delayed tasks in order to shorten the critical path and prevent overall project delays. The project manager should determine whether adding the resources will cost less than delaying overall project completion.
- **Overtime:** Scheduling the resources to work overtime may help reduce the timeline in which tasks are completed. This may also impact the sequence in which tasks are completed.

7.4.4 Change Management (Scope Control) Techniques

Another critical element of project management is a change management process (also referred to as change control) to address potential scope creep and/or gold plating. The change management process should be formally communicated and agreed to at the start of the project/engagement.

It is key that team members understand that additional work outside the scope of the project/engagement should not be performed without appropriate approval. Doing additional work without approval can negatively impact the cost, timeline, and even the quality of the project/engagement.

To summarize, the common steps in the change management process include:

- Submitting a change request
- Approval of the request by the project sponsor and/or appropriate parties
- Update of the project plan, including the timeline, resources, and deliverables impacted, based on the approved changes
- Communication of the updated project plan

© Becker Professional Education Corporation. All rights reserved.

MODULE

8 Performing a Detailed Risk Assessment

Part 2
Unit 1

This module covers the following topics from the *CIA examination syllabus*:

CIA Syllabus—Section A: Engagement Planning

5. Complete a detailed risk assessment of each activity under review

   May include but is not limited to:

   a. Recognize how to apply Topical Requirements when completing a risk assessment

   b. Recognize the pervasive financial, operational, IT, cybersecurity, and regulatory risks as they relate to the activity under review

   c. Recognize the impact of emerging risks on the organization

   d. Determine appropriate methods and criteria to evaluate and prioritize identified risks and controls

   e. Recognize the impacts of change of people, processes, and systems on risk

   f. Recognize the impact of different organizational structures and environments on the risk assessment, including centralized versus decentralized, flat versus traditional, and in-person versus remote work

   g. Recognize the impact of organizational culture on the control environment, including individual and group behaviors and tone at the top

1 Understanding the Activity Under Review

Understanding and assessing risk is fundamental in most engagements and is performed by an organization's internal audit function. Typically, internal auditors perform risk assessments in two different contexts. The first risk assessment takes place when the overall internal audit plan is being developed. The second risk assessment takes place when internal auditors are performing individual engagements and carrying out the internal audit plan. This second risk assessment is referred to as a detailed risk assessment and is geared toward the specific requirements of the engagement. Internal auditors develop the engagement objectives, scope, and engagement approach based on the results of a detailed risk assessment of the activity under review.

© Becker Professional Education Corporation. All rights reserved.

Pass Key

A detailed risk assessment serves the purpose of both validating the original purpose of the engagement as established in the internal audit plan while also ensuring that the scope of the engagement is narrowed down to include the most relevant risks requiring mitigation.

1.1 Applicable Global Internal Audit Standards

Requirements **Standard 13.2 Engagement Risk Assessment (Excerpt)**

Internal auditors must develop an understanding of the activity under review to assess the relevant risks. For advisory services, a formal, documented risk assessment may not be necessary, depending on the agreement with relevant stakeholders.

To develop an adequate understanding, internal auditors must identify and gather reliable, relevant, and sufficient information regarding:

- The organization's strategies, objectives, and risks relevant to the activity under review.
- The organization's risk tolerance, if established.
- The risk assessment supporting the internal audit plan.
- The governance, risk management, and control processes of the activity under review.
- Applicable frameworks, guidance, and other criteria that can be used to evaluate the effectiveness of those processes.

Internal auditors must review the gathered information to understand how processes are intended to operate.

1.2 Definitions

The *Global Internal Audit Standards* define the following terms:

- **Activity Under Review:** The subject of an internal audit engagement. Examples include an area, entity, operation, function, or system.
- **Risk Assessment:** The identification and analysis of risks relevant to the achievement of an organization's objectives. The significance of risks is typically assessed in terms of impact and likelihood.

© Becker Professional Education Corporation. All rights reserved.

1.3 Gathering Information to Understand the Activity Under Review

Each internal audit engagement begins with the chief audit executive and the other internal auditors assigned to the engagement gathering information to ensure a thorough understanding of the organization, the activity under review, and the objective of the engagement. The information gathered is critical to ensuring that risks are properly identified and assessed when being used to plan an engagement. For advisory services, a formally documented risk assessment may not be required, depending on the nature of the engagement.

1.3.1 Understanding the Internal Audit Plan

The internal auditor should start an engagement by developing an understanding of the internal audit plan and the specific reasons why the engagement was included in the plan. This includes understanding whether the engagement was identified due to the results of the organization-wide risk assessment or whether it was due to the request of specific stakeholders. If the engagement was included in the plan due to stakeholder request, the internal auditor should seek to understand any stakeholder expectations regarding the objective or scope of the engagement. The internal auditor should also inquire with senior management regarding any changes to an applicable activity or area that may have taken place since the development of the internal audit plan.

1.3.2 Gathering Evidence to Support the Understanding

The goal of gaining an understanding of the activity under review and the overall organization is to help identify risks relevant to the engagement, which informs the internal auditor when establishing the engagement plan. The internal auditor should obtain recently conducted risk assessments to assist with risk identification. Such assessments may include those performed by management. When management provides a recent risk assessment, the internal auditor may use it to assist in the identification of risks but may not rely solely on the risk assessment performed by management. Additionally, the internal auditor may gather and review information such as:

- Risk assessments, workpapers, or communications related to work performed by first or second line functions or external service providers or regulators.
- The organization's strategic plan.
- Documented processes related to governance, risk management, and control processes.
- Detailed operational documentation such as process maps or policies and procedures.
- Authoritative materials and/or applicable laws and regulations.
- The organization's annual reports and public/regulatory filings.
- Information on the organization's risks, including risk registers, risk categories, results of risk monitoring, and the organization's risk tolerance.
- Financial or operational performance results or indicators.
- Documentation related to loss events, instances of fraud, customer complaints, or control breakdowns.

Internal auditors may gather information by conducting interviews or surveys, performing walk-throughs, attending meetings, physical inspection of relevant property, or observing processes in action. Interviews and discussions should be held with individuals at all levels of the organization. Individual process managers may be able to provide different perspectives and insights on relevant risks as compared to an organization's senior management. Both perspectives are critical to performing an effective detailed risk assessment.

© Becker Professional Education Corporation. All rights reserved.

1.3.3 Applying Topical Requirements

Topical Requirements are additional requirements for internal auditors established by The Institute of Internal Auditors that are intended to complement the *Global Internal Audit Standards*. The purpose of a Topical Requirement is to focus on the specific challenges of a topic area and to enhance the consistency and quality of internal auditor performance on engagements. While conformance with the *Global Internal Audit Standards* is universally applicable to all internal audit engagements, conformance with a Topical Requirement is only required when the subject and scope of the assurance engagement align with a specific audit area covered by a published Topical Requirement. Topical Requirements are recommended but not required for advisory services. Examples of areas that may be covered by a Topical Requirement include cybersecurity, third-party, culture, and business resiliency.

Pass Key

Conformance with Topical Requirements is *mandatory*, but only when a specific Topical Requirement that relates to the area covered by an assurance engagement has been published. Topical Requirements are recommended but not required for advisory services.

2 Factors Impacting Risk and Risk Assessment

When the internal auditor performs a detailed risk assessment for an engagement, the engagement begins with a focus on understanding the activity under review. For the risk assessment to be both efficient and effective, the internal auditor must also spend time understanding the organization as a whole. The types of risks that may be relevant to a specific engagement area and the ways in which risk information is gathered may be impacted by the culture and structure of the organization.

2.1 Recognizing the Impact of Organizational Culture

An organization's culture is the foundation for a strong system of internal control. An effective and ethical control environment is key to ensuring that risks are appropriately identified, understood, and managed. The term "tone at the top" is often used to describe the impact of the attitudes and behaviors of senior management on the rest of an organization. When leaders demonstrate, through their words and actions, the importance of minimizing the impact of unplanned risks or unacceptable behavior, the rest of the organization follows suit. On the other hand, when senior management displays behaviors that are inconsistent with the values of the organization, the organization may be more susceptible to the negative impacts of risk.

Some risk factors associated with a poor tone at the top include:

- Setting unrealistic expectations for deadlines, profitability, or efficiency.
- Organizational incentives that are not aligned with organizational values.
- Senior management is not committed to hiring competent individuals to perform key job functions.

A negative organizational culture can lead to a higher susceptibility to risks such as the override of controls or a disregard for the laws and regulations of an industry.

© Becker Professional Education Corporation. All rights reserved.

An organization with a positive culture may exhibit characteristics such as:

- A positive tone at the top.
- Clear communication of expectations throughout the organization.
- Open dialogue and employee engagement.
- Incentives that are aligned with core values.

A positive organizational culture leads to a more robust understanding of potential risks and an openness to address the risks in a way that aligns with the organization's risk appetite.

2.1.1 Impact of Culture on Decision Making

A positive organizational culture leads to effective decision making as it promotes applying an ethical filter to key decisions. When individuals feel the freedom to think and speak freely about the risks of a certain decision, the organization benefits from a fuller consideration of the potential outcomes.

Groupthink is a term used to describe decision making in which loyalty to a group is valued more highly than objective decision making. This can be a symptom of a poor organizational culture where individuals do not think and speak freely about the potential risks associated with a decision but rather seek consensus and agreement with the group.

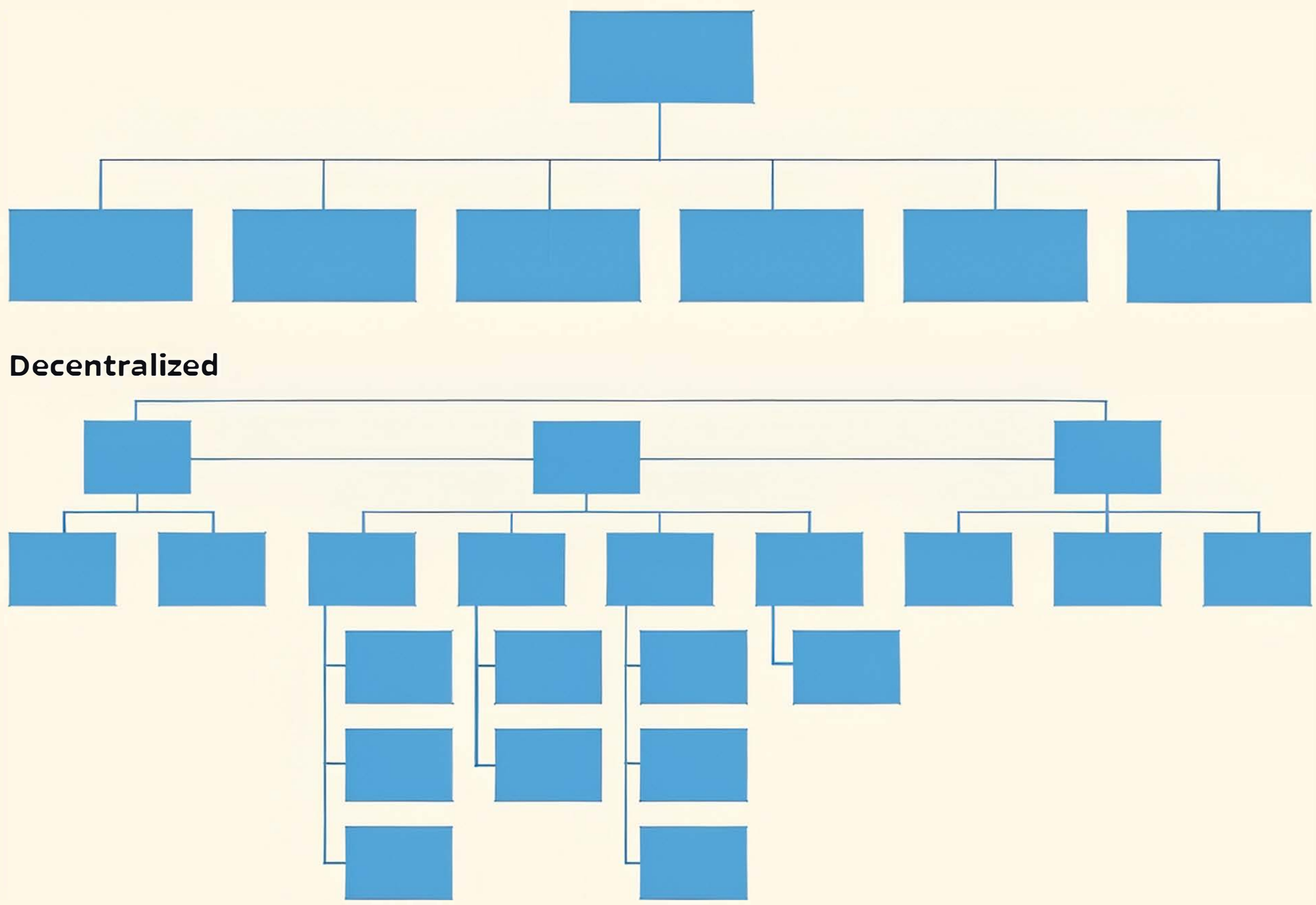
2.2 Recognizing the Impact of Organizational Structure

The organizational structure describes how operational roles and responsibilities are established and carried out on a day-to-day basis. Senior management takes careful consideration when establishing an organizational structure and related policies for its employees. Depending on an organization's structure, new risks may be introduced. Additionally, how management and the internal auditor gather information to support the detailed risk assessment may require amendment to fit the organizational structure.

- **Centralized Versus Decentralized Structures:** A centralized organizational structure tends to have decision making performed by a single individual or small group of individuals (centralized structures are often hierarchical). A decentralized organization distributes decision-making power throughout the organizational levels (decentralized organizations often have flat structures). Centralized structures tend to result in a more consistent application of risk identification and assessment, whereas a decentralized structure may result in a deeper understanding of the unique risks of a particular activity.

© Becker Professional Education Corporation. All rights reserved.

Illustration 1 Centralized vs. Decentralized Organizational Structures



- **Flat Versus Hierarchical (Traditional) Structures:** A flat organization has fewer levels leading to decision making being a collaborative exercise. A hierarchical structure exists when there are multiple levels of management, with the top level being responsible for making the key decision on behalf of the organization. A flat organization may experience a lack of accountability related to risk management and confusion around specific roles and responsibilities. A more hierarchical organization may experience more consistent risk management practices but may suffer from a lack of innovation or employee engagement in many areas, including risk management.
- **Remote Versus In-Person Work:** Individual employees working from remote locations (locations other than an office of their employer) experience an increase in several cybersecurity risks. Remote work introduces IT-related challenges such as an increased number of devices in use, the use of unsecured networks, and the use of unauthorized applications or devices. When organizations have many employees working remotely, risk assessment must be expanded to include the unique risks the working arrangement presents to an organization. Additionally, for the internal auditor to gather information during the detailed risk assessment, it may be more challenging in an environment that has a significant number of employees working remotely.

© Becker Professional Education Corporation. All rights reserved.

3 Identifying and Defining Risks

3.1 Applicable Global Internal Audit Standards

Requirements **Standard 13.2 Engagement Risk Assessment (Excerpt)**

Internal auditors must identify the risks to review by:

- Identifying the potentially significant risks to the objectives of the activity under review.
- Considering specific risks related to fraud.
- Evaluating the significance of the risks and prioritizing them for review.

Internal auditors must identify the criteria that management uses to measure whether the activity is achieving its objectives.

When internal auditors have identified the relevant risks for an activity under review in past engagements, only a review and update of the previous engagement risk assessment is required.

3.2 Definitions

The *Global Internal Audit Standards* define the following terms:

- **Objective:** What an organization wants to achieve. An organization's objectives define what the organization wants to achieve, and its ongoing success depends on the accomplishment of its objectives.
- **Criteria**: In an engagement, specifications of the desired state of the activity under review (also called "evaluation criteria"). The most relevant criteria should be used in the engagement in order to align with organizational objectives and the activity under review.

3.3 Risk Identification Approaches

The chief audit executive determines the approach for risk identification to be used when performing a detailed risk assessment for an engagement. Risk assessments typically include the consideration of both qualitative and quantitative information. To properly identify the risks to the achievement of objectives, the internal auditor must understand the evaluation criteria used by management in determining whether a specific objective has been met. Typical risk identification approaches include the following:

- A **specific-risk approach** involves the identification of risks associated with each activity under review. It is a bottom-up approach and most effective when performing a detailed risk assessment for an individual engagement. The internal auditor normally discusses the business objectives for the activity under review with relevant members of management to identify risks. The internal auditor gives each audit area a composite risk score based on factors such as impact and likelihood.

© Becker Professional Education Corporation. All rights reserved.

- A **risk-by-process approach** involves the internal auditor considering each separate business process and maps key risks to each process. The internal auditor then determines which processes are most critical to the achievement of objectives and how effectively the risks are being managed. The processes with the highest degree of residual risk are prioritized for inclusion in the internal audit plan.
- A **risk-factor approach** is a top-down approach that looks at high-level conditions, or risk factors, at the organizational level that are common across multiple different activities. Risk factors are not the risk itself, but conditions likely to increase the probability of significant risk consequences. The risk-factor approach is more effective in helping the internal auditor perform an organization-wide risk assessment rather than a detailed risk assessment for a specific engagement as it is performed at the macro level.

Internal auditors may select a specific methodology for identifying risks or may use a hybrid approach involving elements of two or more risk identification approaches.

Risk identification may involve the internal auditor brainstorming about possible risk scenarios that could impact a particular activity under review. Brainstorming is more effective when the individuals participating in the brainstorming exercise focus on one objective at a time. A brainstorming session may be done by the internal auditors alone or may involve individuals throughout the organization who are knowledgeable about the specific process or activity. The participants brainstorm barriers or circumstances that may threaten the achievement of objectives, such as:

- External events
- Poorly designed processes and procedures
- Control or process breakdowns
- Lack of competency or ethics in employees
- Poor use of technology
- Fraud

3.4 Impact and Consideration of Specific Risks

For risk identification and brainstorming practices to be effective, internal auditors must have an awareness of the different types and categories of risks that exist. Some of the common risk areas and related risks include:

- **Financial Risks:** Financial risks arise because of the exposure of an organization to financial losses. Financial risks can be further categorized as asset valuation risks and cash flow risks. Specific financial risks include the following:
  - **Interest Rate Risk:** Interest rate risk represents the exposure of an asset to fluctuations in value in response to changes in interest rates. Interest-bearing securities that carry a fixed rate of interest will increase in value as interest rates fall and will decrease in value as interest rates rise. Responses to interest rate risks may include investment in floating rate securities that will track market rates or the use of derivative instruments, such as interest rate swaps.
  - **Market (Systematic) Risk:** Market, or systematic, risk represents exposure to loss from investing in the market as a whole. An example of market risk is the loss in value of the S&P 500 if a severe economic depression grips the country. An organization may respond to market or systematic risks by entering into derivative transactions or by making decisions to operate or not operate in certain markets based on conditions.

© Becker Professional Education Corporation. All rights reserved.

- **Nonmarket (Unsystematic) Risk:** Nonmarket, unsystematic, or price risk represents exposure to losses in investments in specific companies or industries. An example of nonmarket risk is the risk of the adverse impact on the value of a real estate company that has a major fire at a key property. Nonmarket risks can be effectively mitigated through portfolio diversification or the purchase of insurance policies.
- **Default/Credit Risk:** Default risk exposes creditors to the risk that debtors may not pay, or may not timely pay, the principal and/or interest due on indebtedness, reducing the realizable value of the receivable. Default risk can be mitigated by choosing to lend only to borrowers with a low risk of default or by adjusting the interest rate charged to reflect the risk of the borrower.
- **Liquidity Risk:** Liquidity risk represents the exposure associated with being unable to meet financial obligations due to lacking available cash or the ability to obtain cash. Liquidity can be impacted by customer default risk, a decline in available credit to an organization, or market risk. Organizations may reduce liquidity risk by setting up a line of credit or by maintaining cash reserves adequate to meet liquidity requirements.

- **Operational Risks:** Operational risks arise because of the exposure of an organization's day-to-day operations to failure, inefficiency, or loss. Specific operational risks include the following:
  - Human error resulting from individual carelessness or ineffective training. Human error can be mitigated by supervision and training.
  - Information technology failures such as disrupted communications and interrupted or slow processing. Continuous maintenance of systems and ongoing review of system effectiveness are appropriate responses to the risk of IT failures.
- **Quality Risk:** Quality risk relates to the risk that products are defective. Total quality management programs that address continuous improvement can be effective in mitigating quality risk by focusing organizations on customer satisfaction and effective value delivery.
- **Process Failures:** Process failures relate to the risk that processes in place do not operate as intended or are inefficient. Continuous process improvement programs and defect analysis help mitigate the risk of process failures.
- **IT Risks:** IT risks arise due to the use of technology by organizations to advance the way that they operate and communicate. As technological advances continue, organizations are constantly implementing new or changed systems to experience the benefits. IT risks cover a broad range of topics as they can relate to hardware, software, applications, communications, protocols, change management, and data. Examples of IT risks include:
  - Advances in technology that impact product relevance.
  - Choosing a technological solution (e.g., software program) that is not appropriately aligned with strategic objectives.
  - Data breaches or data loss.
  - Significant system downtime causing delays in decision making or operations.
- **Cybersecurity Risks**: Cybersecurity risks or threats relate to the risk that unauthorized users will gain access to an organization's information assets, such as computers, networks, programs, and data. Cybersecurity threats are on the rise and difficult to identify since they are constantly changing. Assessing cybersecurity risks includes considering which information assets are the most likely targets, who has access to information assets, and the impact on the organization if different types of information assets were accessed by unauthorized parties. The impact of a cybersecurity threat may be financial, operational, or reputational.

© Becker Professional Education Corporation. All rights reserved.

- **Regulatory Risks**: Regulatory risks arise because of new or changing regulations or laws and their impact on an organization's ability to meet its objectives. Examples of regulatory risk may relate to new regulations that significantly delay the launch of a new pharmaceutical drug or changes to data privacy laws that require costly process and policy changes within a health care organization. Organizations mitigate regulatory risks by monitoring for updates and using compliance frameworks to assist with regulatory compliance.
- **Emerging Risks**: Emerging risks arise when the business context, including the economy, markets, competition, etc., changes. Examples of emerging risks include areas such as climate change or artificial intelligence. Because these risks are relatively new and relate to ever-changing conditions, they are not always identified in a timely manner or fully understood by organizational management.

3.4.1 Impact of Change on Risks

Organizations typically experience some level of change with respect to their people, processes, and systems. The ability to effectively identify all relevant risks and fully understand them can be further complicated by change. Organizations and internal auditors are tasked with maintaining an awareness of how the operational landscape of an organization is changing. Considerations include changes to markets, regulations, product offerings, technological advances, employees, and many others. Both the pace and type of change have an impact on risk. The faster the rate of change and the more complex the change, the more risk is increased for an organization. For risks related to organization personnel, a high rate of turnover may result in more instances of human error due to a lack of understanding of processes and controls. The turnover of a key member of senior management may be disruptive to the overall tone at the top as a new perspective and approach to risk is established for the organization. Regardless of the area, change is an unavoidable aspect of an organization's risk management and must be considered by both management and the internal auditor.

Pass Key

An increase in the pace or complexity (or both) of change experienced by an organization typically increases risk.

3.5 Defining and Categorizing Risks

As risks are identified through the risk assessment process, the internal auditor must define and categorize the risk. Defining the risk should involve using language that is consistent with the risk culture of the organization. The key to effectively defining risks includes the application of consistent language to the organization's risks. Defined risks are often expressed in terms of cause and effect.

Once the risks are identified and defined, the internal auditor should categorize the identified risks. Using risk categories helps bring consistency to the process of identifying, discussing, and analyzing risks. If management uses a particular framework with predetermined risk categories, the internal auditor should use the same categories. If no risk management framework is in place, the internal auditor can identify categories such as strategic, operational, compliance, and financial risks. Within each risk category, both internal and external threats should be considered. The identified risks should be mapped to the organization's objectives. Categorized risks are listed in a risk inventory or risk universe.

© Becker Professional Education Corporation. All rights reserved.

An important step in finalizing the listing of identified risks is to validate the risk language with process-level employees. This helps ensure that the risks are defined using terminology that is consistent with the organization and understandable to the employees involved in the process.

Illustration 2 Risk Identification

As a part of the internal audit plan, the internal audit team at a company is performing a detailed risk assessment of the external financial reporting process. To begin the risk assessment process, the internal auditors inquire with management regarding the objective related to the external financial reporting process.

- **Organizational Objective:** On-time delivery/filling of accurate and complete annual financial statements.

To further understand the objective, the internal auditor inquired with management regarding the criteria management uses to determine whether the objective has been met. Based on the information obtained from management, the criteria for evaluating the objective includes:

- **Criterion 1:** Annual financial statements are filed with the Securities and Exchange Commission (SEC) by the annual deadline.
- **Criterion 2:** Lenders receive annual financial statements by the contractual deadline.
- **Criterion 3:** External auditors issue an unqualified opinion on the annual financial statements.

The internal auditor determines that a specific-risk approach is appropriate, obtains the process documentation for the financial reporting process, and performs a walk-through with the financial reporting manager and the controller. Based on the objective, management's objective evaluation criteria, and the information gathered during the walk-through, the internal auditor identified and categorized the following risks:

- **Operational Risk:**
  - Risk 1: A lack of competent personnel within the financial reporting and accounting team (due to turnover or other issues) may result in significant human error within the annual financial statements.
  - Risk 2: System downtime related to the accounting and reporting software may cause delays in the production of the annual financial statements.
  - Risk 3: Personnel may intentionally engage in fraudulent financial reporting to meet deadlines or cover up intentional errors or omissions.
- **Regulatory Risk:**
  - Risk 4: New complex financial reporting regulations may result in delays or errors/omissions in the annual financial statements.

© Becker Professional Education Corporation. All rights reserved.

4 Measuring and Prioritizing Risks

Risk assessment is all about understanding the risks that are most significant to the achievement of objectives. For internal auditors, both inherent and residual risks are important. As the detailed risk assessment is performed as an element of planning an engagement, the measurement and prioritization of risks should be based on inherent risk (i.e., risk before the consideration of controls). This will ensure that the engagement approach includes testing the controls that address the risks that are potentially most impactful to the achievement of objectives.

4.1 Definitions

The *Global Internal Audit Standards* define the following terms:

- **Impact:** The result or effect of an event. The event may have a positive or negative effect on the organization's strategy or business objectives.
- **Likelihood:** The possibility that a given event will occur.
- **Risk and Control Matrix:** A tool that facilitates the performance of internal auditing. It typically links business objectives, risks, control processes, and key information to support the internal audit process.

4.2 Prioritizing Risk Based on Impact and Likelihood

The internal auditor must measure and prioritize the identified risks to plan an effective engagement. There is no established requirement on how the risks are measured, but two common factors to consider are the impact and likelihood of each identified risk. The internal auditor applies professional judgment in determining the potential impact and likelihood of each risk but should also seek to understand management's risk tolerance. It is important that the internal auditor maintain objectivity while also factoring in the considerations of management and possible risk outcomes.

4.2.1 Considering the Potential Impact of a Risk

When considering the potential impact of a risk, the internal auditor must establish the ratings and criteria that will be used to assign a measurement of the impact to each risk. The rating for the impact of a risk may be numerical (e.g., a scale from one to five) or categorical (e.g., low to catastrophic). The criteria must be clearly defined and may be described in different areas, such as legal, compliance/regulatory, reputational, operational, and financial. When measuring impact, the internal auditor should focus on the potential impact over a period, such as one year. It is important that the full exposure of a risk is considered. For example, if a risk event may occur more than once during the period, that should be considered and reflected in the impact rating.

© Becker Professional Education Corporation. All rights reserved.

Risk Impact Scale and Criteria

Impact Description	Impact Score	Regulatory Criteria	Operational Criteria	Financial Criteria
Catastrophic	5	Complex, highly regulated environment with strict enforcement; consequences for noncompliance likely to cause legal liabilities and penalties that may result in partial or complete shutdown. Significant financial and reputational impacts.	One or more business units or entire organization may be unable to operate. Impact on reputation.	Greater than $25 million
Highly Significant	4	Complex regulatory environment; legal liabilities and penalties for noncompliance may receive public attention and have lasting impact financially and reputationally.	Multiple business units may be significantly affected. Organization's ability to operate or serve customers may be severely reduced. Impact on reputation.	$10 million to $25 million
Significant	3	Laws and regulations are consistently enforced. Legal liabilities and penalties for noncompliance are material.	One or more business units may be materially affected. Organization's ability to operate or serve customers may be significantly reduced.	$5 million to $10 million (material)
Moderate	2	Active regulatory environment with small to moderate penalties for noncompliance.	Operational effectiveness and efficiency are moderately damaged.	$1 million to $5 million
Low	1	Regulatory environment is lax or penalty for noncompliance is small.	Operational effectiveness or efficiency could be improved, but operations proceed uninterrupted.	Less than $1 million

Source: The IIA's *Global Practice Guide: Developing a Risk-Based Internal Audit Plan* ©2020, The Institute of Internal Auditors, Inc. Licensed for use.

4.2.2 Considering the Likelihood of a Risk

When considering the likelihood of a risk, the internal auditor must establish the ratings and criteria that will be used to assign a measurement of the likelihood to each risk. Like impact ratings, the rating for the likelihood of a risk may be numerical (e.g., a scale from one to five) or categorical (e.g., very low to very high). The criteria must be clearly defined and may be defined in terms of control effectiveness or process complexity. As there is typically a wide range of possible outcomes for any risk event, the internal auditor should consider the risk outcome used in the measurement of impact when determining a rating for likelihood.

© Becker Professional Education Corporation. All rights reserved.

Risk Likelihood Scale and Descriptions

Rating	Score	Description	Criteria
Very high	5	Likelihood of risk occurring is very high relatively.	Operational processes are complex and controls are not effective.
High	4	Likelihood of risk occurring is high relatively.	Operational processes are complex and some control weaknesses are noted.
Moderate	3	Likelihood of risk occurring is moderate relatively.	Operational processes are moderately complex; minor control weaknesses are noted.
Low	2	Likelihood of risk occurring is low relatively.	Operational processes are not complex; controls are effective.
Very low	1	Likelihood of risk occurring is very low relatively.	Operational processes are not complex. Controls are effective.

Source: The IIA's *Global Practice Guide: Developing a Risk-Based Internal Audit Plan* ©2020, The Institute of Internal Auditors, Inc. Licensed for use.

4.2.3 Finalizing the Risk Assessment

The final step of the risk assessment is to combine the impact of the risk ratings for both impact and likelihood. The combined rating is referred to as a risk score. The risk score can be calculated by simply adding up the numbers assigned to each risk rate to come up with a combined rating, or the calculation may be more complex. When the internal auditor determines that some factors are more significant to the achievement of objectives than others, those risk ratings may be weighted to reflect the significance.

Regardless of the approach, the risk assessment should result in a listing of risks with a risk score that can be used for prioritizing or ranking the risks for planning purposes. Risk ranking is often depicted in a heat map format for easy visualization of how the risks compare.

© Becker Professional Education Corporation. All rights reserved.

Illustration 3 Risk Assessment

The internal audit team at a company is performing a detailed risk assessment for the risks identified related to the external financial reporting objective of the company related to the operational risks.

Operational Risks:

- Risk 1: A lack of competent personnel within the financial reporting and accounting team (due to turnover or other issues) may result in significant human error within the annual financial statements.
- Risk 2: System downtime related to the accounting and reporting software may cause delays in the production of the annual financial statements.
- Risk 3: Personnel may intentionally engage in fraudulent financial reporting to meet deadlines or cover up intentional errors or omissions.

To perform the risk assessment, the internal auditor establishes the following risk rating criteria related to the impact and likelihood of the risk:

Operational Impact Criteria:

- Low (1)—operational effectiveness and/or efficiency proceed uninterrupted.
- Moderate (2)—operational effectiveness or efficiency are moderately damaged.
- Significant (3)—organization's ability to operate or serve customers may be significantly reduced.

Operational Likelihood Criteria:

- Low (1)—risk occurrence is unlikely (less than 10 percent).
- Moderate (2)—risk occurrence is moderately likely (between 11 and 50 percent).
- High (3)—risk occurrence is likely (greater than 50 percent chance).

All risk factors will be weighted equally in determining the overall risk score:

	Impact Rating	Likelihood Rating	Overall Risk Score
Risk 1	2	1	3 (Mod)
Risk 2	3	2	5 (High)
Risk 3	3	1	4 (Mod)

Risk Score: 1–2 (Low), 3–4 (Moderate), 5–6 (High)

Based on the professional judgment of the CAE, the resources available, and the engagement objective, all three risks **will** be included in the engagement plan as they are all moderate risk or above. The internal audit team **will** proceed with developing a risk and control matrix, assessing the design adequacy of identified controls, and testing operating effectiveness.

© Becker Professional Education Corporation. All rights reserved.

Typically, risks that fall into the high or moderate risk categories would be included in the scope of an engagement, but other factors play a role in this determination, such as the internal audit charter, resource limitations or considerations, and individual engagement objectives. The CAE should meet with members of senior management to ensure that there is a mutual understanding of the results of the risk assessment and to address any significant differences in risk perceptions.

4.2.4 Developing a Risk and Control Matrix

The information and evidence gathered during a detailed risk assessment are key components of a risk and control matrix. The internal auditor often uses a risk and control matrix to facilitate an effective engagement process. A risk and control matrix combines information regarding management's objectives and the identified risks determined to be an engagement priority through the risk assessment process. The internal auditor then identifies key controls in the organization's business processes that have been designed and implemented to address or mitigate the risks.

The risk and control mapping, as documented in the risk and control matrix, helps to inform the detailed engagement approach and plan. As the engagement progresses, additional information is often documented in the risk and control matrix, including control type, risk consequence, and residual risk assessment.

© Becker Professional Education Corporation. All rights reserved.

MODULE

9 Engagement Procedures

Part 2
Unit 1

This module covers the following topics from the *CIA examination syllabus*:

CIA Syllabus—Section A: Engagement Planning
6. Determine engagement procedures and prepare the engagement work program *May include but is not limited to:* a. Determine procedures to evaluate control design b. Identify procedures to test the effectiveness of controls c. Identify procedures to test the efficiency of controls d. Evaluate the adequacy of the engagement work program e. Identify testing methodologies for an engagement that includes accounting, finance, IT systems, business operations, or cybersecurity

1 Procedures for Evaluating and Testing Controls

1.1 Determining Control Procedures During Planning

Evaluating the adequacy of control design is part of the planning phase of the engagement process. This occurs after the engagement objectives and scope have been determined, an understanding of the activity under review has been obtained, risks have been identified and assessed, and key controls have been identified. Internal auditors will then evaluate the adequacy of the control designed to determine whether the controls, if operating effectively, will mitigate the risks that could prevent the achievement of objectives.

After the adequacy of the control design is completed, procedures for testing the operating effectiveness and efficiency of controls will be identified and included in the engagement work program. This is part of the planning phase, which also includes allocating engagement resources. The testing procedures are executed in the performing services (conducting engagement work) phase of the engagement process.

1.2 Control Design Adequacy

Evaluating the adequacy of control design can be performed during engagement planning. This step helps internal auditors identify key controls to test for operating effectiveness. However, the control design evaluation may occur at a specific point of the engagement or while performing the test of the effectiveness of controls. The timing depends on the nature of the engagement.

The evaluation of whether internal controls are adequately designed includes obtaining an understanding of the control design and performing procedures to evaluate the adequacy of control design.

© Becker Professional Education Corporation. All rights reserved.

1.2.1 Evaluating the Adequacy of Control Design

The purpose of evaluating control design adequacy is to determine whether key controls are designed to effectively reduce the risks of the process to an acceptable level. Internal auditors should consider the following when determining procedures for evaluating the adequacy of control design:

- Acceptable level of risk based on the organization's risk tolerance level
- Appropriateness and sufficiency of key controls to address risks
- Existence of compensating controls
- Adequacy of process design
- Existence of gaps in the design and their root causes, including possible impacts

Internal auditors can use multiple procedures to understand the control system, including discussing with management and reviewing organizational plans, policies, and processes.

Internal auditors can also directly observe a process by performing walk-through procedures to trace the flow of the control processes, gain an understanding of the design of internal controls, and eventually evaluate their design adequacy. Walk-through procedures may include inquiry, observation, and inspection.

- **Inquiry**—inquiring of those who perform the control procedures and obtaining their verbal or written responses. Inquiries generally include:
  - The individual's understanding of the control procedures.
  - Whether controls are performed as required and on a timely basis.
  - Situations in which the individual and others do not perform the required control procedures.

  Inquiry may take the form of interviews, surveys, and questionnaires. However, inquiry alone is not sufficient as it produces indirect evidence, particularly when the individuals being questioned may provide biased responses. Internal auditors should corroborate inquiry responses by performing additional procedures.
- **Observation**—watching individuals perform the control procedures. This can be more convincing than inquiry because internal auditors obtain evidence through direct observation.
- **Inspection**—reviewing documents and records or physically examining tangible resources (e.g., inventories, equipment), providing direct knowledge to internal auditors of the existence and condition of evidence.

© Becker Professional Education Corporation. All rights reserved.

1.2.2 Documenting the Evaluation of Control Design Adequacy

Once the evaluation is completed, internal auditors should document their observations and conclusions and then discuss with management if design gaps are identified. A risk and control matrix can be a useful tool for documentation and communication in this regard.

Based on the evaluation results of control design adequacy for each process-level risk, internal auditors can assess the overall design adequacy of the process as a whole. Conclusions drawn from such evaluation may include:

- The overall process design is adequate to manage the risks to an acceptable level.
- The overall process design is adequate to manage the risks to an acceptable level. However, the existence of certain gaps may lead to some risk exposure the process owner may find unacceptable.
- The overall process design is not adequate to manage the risks to an acceptable level. Significant gaps exist, creating an intolerable level of risk exposure that impedes the achievement of objectives.

As directed by the Standards, the evaluation of the adequacy of the control design should be documented in either the work program or a separate workpaper.

Pass Key

Procedures to evaluate control design adequacy should focus on determining whether the controls are designed to effectively reduce the risks of the process to an acceptable level.

1.3 Control Effectiveness

After evaluating the adequacy of the control design, the next step is to develop a test plan and identify procedures for gathering sufficient and appropriate evidence to test the operating effectiveness of key controls. By evaluating both the design and the operational effectiveness of controls, internal auditors gain reasonable assurance that the process **will** meet its objectives.

The procedures for testing the effectiveness of controls include obtaining evidence regarding:

- whether the controls were applied at relevant times;
- how controls were applied;
- the consistency with which controls were applied; and
- by whom or by what means controls were applied.

© Becker Professional Education Corporation. All rights reserved.

1.3.1 Which Controls to Test

While internal auditors may test all the identified key controls, they also need to consider other factors when deciding which controls to focus on to optimize resources:

- **Higher-Level Controls:** Internal auditors should consider whether high-level controls, such as monitoring or supervisory controls performed by supervisors, provide reasonable assurance that the relevant risks are managed sufficiently.
- **Compensating Controls:** Testing compensating controls that address multiple risks may be more efficient than simply testing each of the key controls.
- **Control Design Adequacy:** If the design of the controls is inadequate, it may not be necessary to test the effectiveness of those controls. Internal auditors may also determine how to assess the impact of errors from inadequate control design.
- **Timing of Controls:** Internal auditors should consider whether it is practical to test the controls during the engagement period. For instance, for controls operating only at year-end, it may not be practical to test them for engagements conducted during the year.
- **Changes in the Process:** Consider changes in processes that might influence how key controls operate, which may affect how the controls are tested.

Internal auditors' judgment is used to determine the testing approach, which includes the nature, extent, and timing of tests of key controls. The testing approach can be documented in the risk and control matrix and the procedures included in the engagement work program.

1.3.2 Nature of Tests

The type of test determines the level of assurance and the amount of time required to perform it. Tests of control effectiveness, presented in the order of the evidence that they would ordinarily produce, from least to most, include the following: inquiries, observation, inspection, vouching, tracing, and reperformance. Internal auditors should use a combination of procedures to obtain sufficient evidence of operating effectiveness.

Documentation may provide evidence of operating effectiveness for some controls; for other controls (such as the assignment of responsibility or segregation of duties), documentation may not be available or relevant. To test such controls, the internal auditor would likely rely on inquiry and observation.

Pass Key

Internal auditors perform procedures to evaluate control effectiveness, which include asking appropriate personnel questions, observing operations, inspecting relevant documentation, and reperforming the control process.

Inquiry alone is not sufficient. Observation generally is pertinent only at the time the observation is made, so observation should be supplemented with other procedures, such as inquiry, inspection, and reperformance.

© Becker Professional Education Corporation. All rights reserved.

1.3.3 Extent of Tests

Key controls can be tested partially (i.e., a sample of transactions) or completely (i.e., the entire population of transactions). The more extensively a control is tested, the greater the evidence obtained. However, more extensive testing also takes more time and effort. Internal auditors should consider the following factors in determining the appropriate extent of tests:

- The frequency of the performance of the control during the period.
- The relevance and reliability of the evidence to be obtained.
- Whether it is necessary to obtain evidence about the effective operation of indirect controls (e.g., general IT controls) that support the operation of other controls.
- If a control is applied on a transaction basis throughout the period, using sampling to test the control may be appropriate.

1.3.4 Timing of Tests

The timing of tests depends on the period covered in the engagement's scope, the nature of the control, and the type of test performed.

1.4 Control Efficiency

To evaluate the efficiency of controls, the internal audit function typically assesses whether management actively measures and monitors the associated costs and benefits of control processes. The evaluation involves:

- Determining if resources consumed in the control process, such as time, personnel, technology, and financial investment, are justified by the benefits they provide in mitigating risks, improving operations efficiency, and achieving business objectives.
- Identifying whether resources allocated to the control processes are being used optimally and whether they align with the organization's strategic objectives.
- Examining if the control processes inadvertently introduce significant business concerns regarding operational inefficiencies, excessive complexity, or unintended consequences. This may include errors due to redundant or poorly designed control processes, delays in decision making due to excessive bureaucracy, or duplication of efforts across teams.
- Benchmarking controls performance by comparing efficiency in one area of the organization to another area of the organization.
- Considering the possibility of overcontrol, such as excessive control in low-risk areas, controls that unnecessarily hinder the performance of basic employee responsibilities, and redundant controls.

Procedures used for such evaluations may include inquiry, observation, and inspection. Analytical procedures may also be implemented to perform cost-benefit analysis to assess control efficiency.

© Becker Professional Education Corporation. All rights reserved.

2 Engagement Work Program

Requirements **Standard 13.6 Work Program**

Internal auditors must develop and document an engagement work program to achieve the engagement objectives.

The engagement work program must be based on the information obtained during engagement planning, including, when applicable, the results of the engagement risk assessment.

The engagement work program must identify:

- Criteria to be used to evaluate each objective.
- Tasks to achieve the engagement objectives.
- Methodologies, including the analytical procedures to be used, and tools to perform the tasks.
- Internal auditors assigned to perform each task.

The chief audit executive must review and approve the engagement work program before it is implemented and promptly when any subsequent changes are made.

2.1 Developing the Work Program

Developing a work program and allocating resources to the engagement are the final steps in the planning phase of the engagement process. When planning an engagement, internal auditors collect and organize information to create an engagement work program. The work program builds on the details gathered during engagement planning.

As defined in the *Global Internal Audit Standards*, an engagement work program is a "document that identifies the tasks to be performed to achieve the engagement objectives, the methodology and tools necessary, and the internal auditors assigned to perform the tasks." The work program guides the analysis and evaluation of information as internal auditors develop findings, recommendations, and conclusions.

To develop a work program, internal auditors need to have a comprehensive understanding of the engagement's objectives and scope, including the key risks and controls within the activity under review. For advisory engagements, the work program should be developed in collaboration with the stakeholders who requested the advisory services.

Additionally, internal auditors may need to consider the following key factors of the upcoming engagement before developing the work program:

- Determining the appropriate sample size for testing and selecting suitable methodologies
- Reviewing the risk register or risk matrix and its relevance to the work program's development
- Identifying strategies to achieve the engagement objectives
- Assessing the availability of necessary resources

© Becker Professional Education Corporation. All rights reserved.

The work program can be developed by connecting the risks and controls identified during the risk assessment with the planned testing approach. As the engagement progresses and analyses are conducted, internal auditors can further connect these risks and controls to their findings and conclusions.

As mentioned in the Standards, the level of detail and analysis employed in the planning phase varies based on the internal audit function and the specific engagement. When sampling is used, the work program should always specify the sampling methodology, population, sample size, and whether the sample results can be reliably projected to the entire population.

2.2 Adequacy of the Work Program

Determining the adequacy of the work program depends on the nature, extent, and timing of procedures needed to meet engagement objectives and must be based on the information obtained during engagement planning, including engagement risk assessment, when applicable.

Each procedure included in the work program should target a specific control that mitigates a particular risk. Additionally, the work program should be developed and documented clearly to allow all engagement team members to understand their responsibilities and to track outstanding tasks.

As outlined in the Standards, the engagement work program must identify:

- Criteria to be used to evaluate each objective
- Tasks to achieve the engagement objectives
- Methodologies, including the analytical procedures to be used, and tools to perform the tasks
- Internal auditors assigned to perform each task

Also, the adequacy of the work program can be evaluated against the satisfaction of the following criteria:

- Whether it clearly specifies the engagement work and program objectives
- Whether it appropriately summarizes the engagement work to be performed to enhance understanding of the activity under review
- Whether it demonstrates that the work has been adequately planned
- Whether it facilitates review by supervisors who oversee the engagement planning process
- Whether it provides assurances that all significant risks have been considered
- Whether it aids in managing tasks and assigning responsibilities effectively
- Whether it brings structure and clarity to the engagement process
- Whether it ensures that conclusions are aligned with the engagement objectives

Every work program must be approved by the CAE, or designee, before the start of engagement fieldwork. Should it become necessary to make adjustments to the work program due to new information and knowledge obtained during fieldwork, the changes are subject to prompt approval by the CAE.

© Becker Professional Education Corporation. All rights reserved.

2.3 Format of the Work Program

Work completed during engagement planning should be documented in workpapers and referenced in the work program. The format of the work program varies with the nature of the engagement or the requirements of the organization. Commonly used formats include:

- Standard templates or checklists to track the completion of planning steps, which are often used to ensure the completeness of necessary tasks to be covered in the engagement.
- Memoranda summarizing completed tasks, typically used in cases where dynamic planning is required from engagement to engagement and a free-form approach is more appropriate.
- Additional columns in the risk and control matrix when it is more desirable to capture everything in one document.
- A combination of the three.

Regardless of the format, a well-documented work program helps communicate roles, responsibilities, and tasks to the engagement team. It often includes sign-offs for completed work, the names of the internal auditors who conducted the work, and the dates the work was finalized. It should also include an indication of review and approval by supervisors of the tasks completed.

To sum up, a typical work program should cover the following elements:

- Planning tasks (e.g., understanding the process, assessing process-level risks, identifying key controls)
- Field tasks, including specific tasks to be performed
- Key administrative tasks (e.g., preparation of a planning memo, establishing key milestones)
- Key meetings (e.g., kick-off meeting with the management of the activity under review to discuss engagement objectives, scope, timeline, information needed, final deliverables, management's expectations)
- Wrap-up steps (e.g., clearing open review notes, finalizing workpapers, and conducting closing meeting with management)
- Reporting tasks (e.g., preparing draft engagement communication, gathering feedback from management, delivering final engagement communication)

Pass Key

As noted in the Standards, "internal auditors must develop and document an engagement work program to achieve the engagement objectives."

© Becker Professional Education Corporation. All rights reserved.

3 Testing Methodologies for an Engagement

According to the Standards, the testing methodologies for performing procedures must be identified in the engagement work program. This can include the analytical procedures to be used and the sampling methodology when sampling is used. Common testing methods used in internal audit engagements include inquiry, observation, inspection, and reperformance.

Controls may be classified as preventive or detective based on the intent of their implementation. Controls may also be manual or automated depending on how the control process is carried out by the organization. Controls may also be grouped based on whether they are performed at the organization, process, or transaction level. A single control may fall into more than one of these categories.

Different types of controls may be tested, including:

- **Segregation of Duties:** Strong policies are in place to ensure different employees are responsible for authorization, recording, and custody functions within a given business process.
- **Policies and Procedures:** Documentation indicates the series of steps to be performed for a given task or provides guidance for decision making in different circumstances to ensure quality and efficiency of work.
- **Authorization/Approvals:** Certain actions require the approval to take place (e.g., there may be a policy in place indicating department heads cannot spend over $50,000 without controller approval).
- **Reconciliation:** Records and supporting documentation are reconciled on a routine basis (e.g., the cash accounting records are compared with bank records to determine whether adjustments should be made).
- **Management Review:** On a routine basis, management reviews the work of the subordinates or the results of business activities (e.g., the quality assurance department reviews deviations from product specifications for the month to determine root causes).
- **IT Controls:** Application controls and general IT controls are established.
- **Physical Security:** Access to tangible assets, intellectual property, and sensitive information is protected.
- **Training:** Employees and contractors are provided with adequate training to perform their job functions with sufficient quality and efficiency.

© Becker Professional Education Corporation. All rights reserved.

Example 1 Controls and Testing Methodologies

Control Description	Testing Methodology
Segregation of Duties No employees will have the authority to both initiate sales orders and approve new customers or set credit limits.	• To test the design of the control, the internal auditor obtained and inspected the policy to ensure this segregation of duties is documented. • To test the operating effectiveness, the internal auditor selected a sample of sales orders and inspected it to determine the employee who initiated it and separately obtained the respective customer approval file noting that the customer was approved and the credit limit was set by an authorized employee in the credit risk department, separate from the sales team.
Policies and Procedures The Patient Intake Policy dictates the information and documents required to accept a patient at the clinic and must be followed by all medical receptionists.	• To test the design of the control, the internal auditor obtained and inspected the policy to determine whether it is adequately designed to meet regulatory (i.e., HIPAA), insurance, and clinic objectives. Additionally, the internal auditor observed the policy posted at the reception desk and inquired of medical receptionists regarding its use. Finally, the internal auditor observed the patient intake process for a new patient, noting whether all required information and documents were requested. • To test the operating effectiveness, the internal auditor selected a sample of patient files for patient appointments in the past month and inspected to determine whether all required information and documents were present in the file.
Authorization/Approvals All purchase orders (POs) greater than $10,000 require controller approval prior to release.	• To test the design of this control, the internal auditor inquired of the procurement department and observed a dummy PO in the amount of $10,000 being generated in the procurement application, noting that the system flagged it for further review and approval. • To test the operating effectiveness, the internal auditor selected a sample of released POs that varied in amount, noting whether approval was required and, if so, whether there was evidence of the controller's approval.
Reconciliation On a monthly basis, the accounts receivable subledger is reconciled with the AR account in the general ledger to ensure invoices, payments, and any credit memos are appropriately reflected.	• To test the design of this control, the internal auditor observed the AR clerk performing the control and performed corroborative inquiry with the AR Manager. • To test the operating effectiveness, the internal auditor reperformed the reconciliation for a number of months in the period under audit.
Management Review The accounting manager reviews the budget-to-actual analysis on a monthly basis, obtaining and documenting explanations for all budget items with deviations greater than 5% and $50,000.	• To test the design of this control, the internal auditor inquired of the controller regarding the review process and observed one month's budget-to-actual analysis as it was performed. • To test the operating effectiveness of the control, the internal auditor obtained the budget-to-actual analysis for a sample of months in the period and inspected it to determine whether explanations were obtained for all variances greater than 5% and $50,000. Corroborative inquiry was performed regarding a sample of explanations to determine their appropriateness, vouching and tracing to supporting evidence (e.g., POs, invoices, and proofs of payment) where necessary.

(continued)

© Becker Professional Education Corporation. All rights reserved.

(continued)

IT Controls System privileges are granted by job title.	• To test the design of this control, the internal auditor obtained and inspected the approved system privileges for all job titles in the organization and inquired of the system administrator. Additionally, the internal auditor with IT specialization observed the configuration in the system to determine whether it reflected the approved documentation. Separately, the internal auditor observed an employee outside of IT fail to access a module outside of their privileges, consistent with the configuration. • To test the operating effectiveness, the internal auditor selected a sample of employees, obtained their employment files to confirm their job titles, and then inspected their system access, noting whether it reflected their access associated with job titles.
Physical Security Inventory stored in warehouses is secured every evening upon operations shut down.	• To test the design of this control, the internal auditor inquired of facilities personnel regarding locking protocols and the presence of security officers at night. Additionally, the internal auditor observed the nightly lock-up at one warehouse and observed the shift commencement of the security officer. • To test the operating effectiveness of the control, the internal auditor selected a sample of warehouses to visit. For each warehouse, the internal auditor checked all external doors after operations shut down and also observed and inquired of security officer personnel.
Training All new employees are required to attend instructor-led cybersecurity training.	• To test the design of this control, the internal auditor obtained and inspected presentation materials evidencing the training and inquired of human resources regarding training tracking and requirements. • To test the operating effectiveness, the internal auditor took a sample of employees hired in the past year and obtained and inspected their employee files, noting they all appropriately registered for cybersecurity training. The internal auditor also obtained sign-in documentation evidencing actual attendance for each training offered and traced it back to employee file training registrations.

3.1 Accounting and Finance Systems

For an engagement that involves accounting and finance systems, internal auditors should perform tests to evaluate the design and implementation of controls that address risks of financial information processing and recording. Internal auditors may use testing methodologies that involve inspection of documents, reperformance, analytical procedures, and sampling.

Internal auditors can assess the control design and effectiveness regarding accounting and finance systems by focusing on controls of authorization, custody, and recording regarding the following cycles:

- Sales-receivables cycle
- Cash receipts cycle
- Purchase-payables cycle
- Cash disbursements cycle
- Payroll cycle

© Becker Professional Education Corporation. All rights reserved.

3.2 Business Operations

Controls in business operations include a combination of manual controls and automated controls. Internal auditors should evaluate the design and implementation of these business operation-related controls using testing methods such as inquiry, observation, including walk-throughs, inspection, and sampling.

3.3 IT Systems

IT-specific controls can also include general IT controls and information-processing controls related to IT applications. Internal auditors should develop tests to evaluate the design and implementation of these IT-related controls using testing methods such as inquiry, inspection, reperformance, and sampling.

- **General IT Controls**

  General IT controls are policies and procedures that relate to many applications and support the effective functioning and proper operation of the information system and the integrity of information in the entity's information system. Internal auditors first obtain an understanding of the risks arising from the entity's use of IT and then identify the general IT controls put in place to address such risks. General IT controls address the risks arising from the use of IT and can be categorized as:

  - **Applications**—correlate to the nature and extent of application functionality and integration.
  - **Database**—address risks arising from the use of IT related to unauthorized updates to information in the database.
  - **Operating System**—address risks related to the use of IT related to administrative access, which can facilitate the override of other controls.
  - **Network**—address risks arising from the use of IT related to network segmentation, remote access, and authentication.

- **Information-Processing Controls**

  Information-processing controls can be automated or manual and are applied to the processing of information and transactions, and can help to ensure that transactions occurred, are authorized, and are completely and accurately processed and reported. Such controls help to ensure the integrity of the data in an entity's information system. Controls over input, processing, and output include:

  - Controls over interfaces, integrations, and e-commerce
  - Checking the mathematical accuracy of records and reports
  - Maintaining and reviewing accounts and balances
  - Automated edit checks of input data
  - Manual follow-ups of exception reports
  - Controls over the use of emerging technologies such as blockchain, robotics, or artificial intelligence

© Becker Professional Education Corporation. All rights reserved.

3.4 Cybersecurity

Cybersecurity controls include the combined force of policies, processes, tools, and personnel to safeguard an organization's information resources. These controls work together to achieve the following objectives:

- Protecting information assets from various types of cyberattacks
- Detecting and identifying cybersecurity incidents as they occur
- Effectively remediating security vulnerabilities and deficiencies to minimize damage and prevent recurrence

Effective controls to address cybersecurity risks may involve:

- Robust security frameworks
- Detecting and addressing top risks related to cybersecurity
- Deploying cybersecurity awareness programs for employees
- Considering external and internal threats when designing the cybersecurity program
- Strong governance over information security within the organization
- Effective response protocol in response to serious cybersecurity breaches

3.4.1 Assessment Methodology

To assess the design and effectiveness of cybersecurity controls and governance, internal auditors can follow the following framework by focusing on six components:

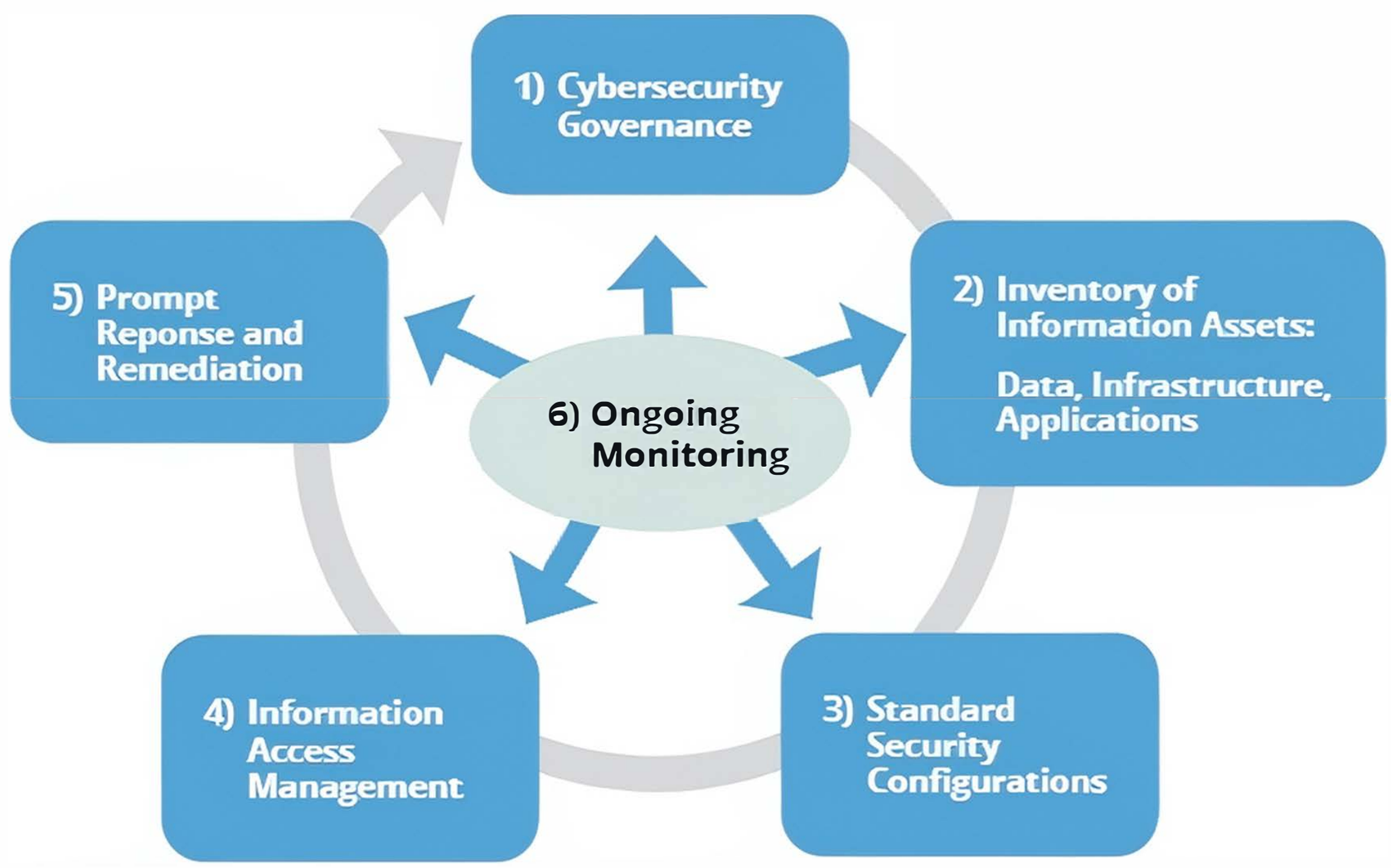
- **Cybersecurity Governance:** Effective governance is reflected in clearly defined policies, relevant tools, sufficient staffing, and insightful training. Stakeholders also play significant roles in strengthening cybersecurity governance. These stakeholders may include a cybersecurity governance committee that includes senior management and representatives from first, second, and third line roles (e.g., technology and process owners and potentially key external stakeholders, such as suppliers, customers, service providers, and peer groups).
- **Inventory of Information Assets:** When assessing information assets, considerations include:
  - data types (e.g., transactional, IT configuration, unstructured), classification, and environments (e.g., data warehouses, key databases);
  - infrastructure such as servers, network devices, and end-user devices;
  - applications; and
  - external relationships, such as third-party hosting and data sharing.

  Organizations must identify and monitor all software and devices interacting on the network, particularly in environments allowing employee-owned devices, to mitigate cyber threats. Effective detection, authentication, and inventory of unknown devices enable better tracking and enhance the overall cybersecurity strategy.

© Becker Professional Education Corporation. All rights reserved.

- **Standard Security Configurations:** Centralized, automated configuration management software helps establish and maintain baselines for devices, operating systems, and applications more effectively than manual or inconsistent methods. Internal auditors should review these baselines to assess risks accurately. Additionally, processes for applying patches and updates are essential to keeping configurations secure as new threats emerge.
- **Information Access Management:** Management should implement preventive controls, such as approving and granting user access based on job roles and adjusting access promptly when employees change roles. Internal auditors can review user access to key data and systems to ensure access is appropriate for current roles. Both internal and external users, including employees, consultants, and vendors, should be closely monitored.
- **Prompt Response and Remediation:** An organization's ability to quickly communicate and address risks reflects the effectiveness and maturity of its program.
- **Ongoing Monitoring:** Continuous auditing of the framework's five components is essential to evaluate risk management and the effectiveness of corrective actions.

Cybersecurity Risk Assessment Framework



Source: The IIA's *Global Technology Audit Guide: Assessing Cybersecurity Risk, The Three Lines Model* ©2020. The Institute of Internal Auditors, Inc. Licensed for use.

© Becker Professional Education Corporation. All rights reserved.

MODULE

10 Engagement Resources and Skills

Part 2
Unit 1

This module covers the following topics from the *CIA examination syllabus*:

CIA Syllabus—Section A: Engagement Planning

7. Determine the level of resources and skills needed for the engagement

   May include but is not limited to:

   a. Determine financial resources required for the engagement

   b. Determine human resources required for the engagement

   c. Determine technological resources required for the engagement

   d. Evaluate implications of resource limitations

1 Planning Engagement Resources

Requirements **Standard 13.5 Engagement Resources**

When planning an engagement, internal auditors must identify the types and quantity of resources necessary to achieve the engagement objectives.

Internal auditors must consider:

- The nature and complexity of the engagement.
- The time frame within which the engagement is to be completed.
- Whether the available financial, human, and technological resources are appropriate and sufficient to achieve the engagement objectives.

If the available resources are inappropriate or insufficient, internal auditors must discuss the concerns with the chief audit executive to obtain the resources.

As outlined in the Standards, internal auditors must identify the types and quantity of resources needed to complete an engagement and fulfill the engagement objectives based on the nature, complexity, and time frame of the engagement as well as the appropriateness and sufficiency of resources. Those resources include:

- Financial resources
- Human resources
- Technological resources

© Becker Professional Education Corporation. All rights reserved.

The engagement supervisor or a lead internal auditor is usually responsible for identifying and assigning resources during the planning phase of the engagement.

Pass Key

As outlined in the Standards, internal auditors must identify the types and quantity of resources required to complete an engagement based on the:

- nature and complexity of the engagement;
- time frame of the engagement; and
- appropriateness and sufficiency of resources.

1.1 Steps to Plan Engagement Resources

There are several steps that an engagement supervisor may take during engagement planning to help identify and allocate required resources for the engagement (financial resources, human resources, and financial resources).

1.1.1 Budget/Estimate

Internal auditors should budget or estimate resources, including the number of hours and costs required to conduct the engagement. Typically, an internal auditor with prior experience budgeting and estimating resources leads this process.

- **Number of Hours and Human Resources (Human Resources Required for the Engagement)**

  When determining the human resources needed for the engagement, the number of hours to meet the engagement objectives, the types of services to be performed (including any services requiring specialized skills or knowledge), and the time frame of the engagement should be considered.

  The number of hours needed to complete the assignment may be estimated based on past engagements and the experience of the internal auditors performing the services. The estimated hours should account for the entire engagement duration, including hours needed for the planning, performing, and communication phases of the engagement. The use of technological tools and resources may also impact the number of hours needed by internal auditors.

  While the estimated hours **will** not be exact, the estimate should be realistic. However, there may be unexpected events impacting the engagement timeline and/or resources. For example, it is possible that an internal auditor becomes ill or leaves the organization during the engagement. Often, these types of circumstances cannot be predicted in advance.

  Also, if the engagement needs to be completed in a short time frame, that may require more human resources to be allocated to the engagement in order to meet the deadline.

  After considering the availability of internal resources, the internal audit function can determine whether outside service providers are needed to supplement skills and/or time based on the estimated number of engagement hours and the nature of services to be performed.

© Becker Professional Education Corporation. All rights reserved.

- **Technological Resources (Required for the Engagement)**

  There may be technological tools and resources that can help internal auditors perform the engagement more efficiently and effectively. These can include tools that assist with data analytics to enable the analysis of historical and current data, artificial intelligence (AI) and machine learning, and robotic process automation (RPA).

  There may also be specific risks arising from technology that need to be addressed as part of the engagement, requiring the use of service providers with specialized skills and knowledge.

  The impact of technological resources required for the engagement impacts the financial and human resources required as well.

- **Costs (Financial Resources Required for the Engagement)**

  In addition to the cost of human resources, internal auditors should include other financial costs needed to complete the engagement in their cost estimate. Examples of other costs include:

  - Travel and related expenses

    There may be a need for internal auditors to travel to perform their work away from the internal auditor's location, such as visiting a warehouse located in a remote place or traveling to various branches to conduct the work.

  - Technology costs (also impacting technological resources needed for the engagement)

    The internal audit function may need to access unique or nonroutine technology, such as data analysis and network security analysis software, to complete the engagement. The costs associated with technology should be included in the cost estimate. If the budget does not allow for the use of needed technology, that may impact the ability of the internal audit function to perform the engagement or may impact the need for additional human resources.

  - Supplies and other nonroutine items

    The cost estimate should be all-inclusive, which means capturing all expenses expected for the engagement, including expenses such as costs of supplies and other nonroutine items needed for the engagement.

    For example, internal auditors may need special types of shoes or clothing when observing or performing inventory counts at a factory or warehouse. Another example of a miscellaneous cost may be the cost of printing and distributing final deliverables.

1.1.2 Assemble and Allocate Human Resources

Once the engagement budget (for human resources, financial, and technological resources needed) is determined, the engagement team is assembled, and the human resources needed for the engagement are allocated.

Allocating human resources is often the most challenging aspect of this step. An internal auditor responsible for allocating resources may use the steps described in an engagement work program to allocate human resources.

© Becker Professional Education Corporation. All rights reserved.

When allocating human resources, the internal auditor should exercise professional judgment and consider the following points in the process:

- Types of skills and competencies needed to complete the engagement

  In addition to technical knowledge, other skills or competencies needed to complete the engagement should be considered, such as a language requirement. The CAE should understand the competencies of internal auditors, as it is the CAE's responsibility to evaluate their competencies. Based on Standard 10.2, the CAE may consider the following factors:

  - Previous experience required for the engagement
  - Who in the department has the skills, competencies, and experience needed for the engagement
  - Any special skills that are needed for the engagement but do not exist internally
  - Any professional development aspect that impacts resource allocation
  - Any other unique departmental matters that may impact resource allocation for the engagement

Some internal auditors may need certain experience for their professional development. Standard 10.2 requires the CAE to collaborate with internal auditors to help develop their individual competencies through training, supervisory feedback, and/or monitoring.

The internal auditors may use an engagement work program to allocate human resources based on steps described in the program. The considerations above also help internal auditors identify if there is a need for the internal audit function to engage third-party vendor services. This includes identifying a need for subject matter experts for a specific engagement.

1.1.3 Schedule Human Resources

After assembling and allocating appropriate human resources for the engagement, it is time to schedule those resources. Scheduling human resources is a dynamic process, and internal auditors should consider possible constraints with human resource allocation and scheduling. The internal auditors should secure the availability of the following:

- **Key Process Personnel**

  Internal auditors should consider the timing of an internal audit engagement around the availability of key process personnel. Certain times of the month or quarter may be inconvenient for the personnel. Internal auditors should also consider whether there are other projects that the personnel need to prioritize over the internal audit engagement, which may impact the personnel's availability.

  Internal auditors should be aware of other scheduling issues for key personnel, such as vacation, training, and travel, when the personnel may be limited and/or not available to assist the engagement.

- **Engagement Resources**

  Similar to key process personnel, internal auditors may have other commitments that could impact the scheduling of the engagement.

- **Outside Resources**

  If the internal audit function plans to utilize outside resources, such as a third-party vendor that offers special skills, the availability of those resources must be considered. They might follow a different schedule from the organization and/or acknowledge different holidays. This may be particularly important if the internal audit function plans to engage with a vendor who is in a different country from the organization.

© Becker Professional Education Corporation. All rights reserved.

- **Key Reviewers**

  Securing the availability of key reviewers, such as the internal audit manager or internal audit director, is as important as the availability of other resources noted above. Without key reviewers to review the engagement work, the completion of the engagement may be delayed.

1.2 Other Resource Considerations

1.2.1 Resource Limitations

The internal audit function may face resource limitations, such as constraints in the availability of human resources, time, budget, or technology, which may prevent the internal audit function from achieving the engagement objectives.

As noted in the Standards, in situations where the available resources are inappropriate or insufficient to complete the engagement, the engagement supervisor is responsible for escalating the concern to the CAE. Once the matter is escalated, the CAE is responsible for discussing it with senior management and the board.

As required by the Standards, the CAE must communicate with the board and senior management regarding the appropriateness and sufficiency of the internal audit function's financial, human, and technology resources. The CAE should discuss the implications of resource limitations with them and determine what action to take to resolve the resource challenge.

The CAE may need to consider reducing the scope of the engagement if the internal audit function is unable to secure sufficient and appropriate resources for the engagement.

Illustration 1 Impact of Human Resource Limitation

A small internal audit team is actively in the planning phase of an engagement for a high-risk area with an eight-week deadline for completion. One of the team's auditors, specifically the engagement supervisor, unexpectedly went on medical leave, leaving insufficient staff on the team to complete the engagement within the timeline.

The CAE considers the options:

- Hiring external consultants
- Reducing the scope
- Reallocating internal resources

Given the team's size and budget constraints, the CAE decided to assign the engagement to another auditor; however, the CAE managed the overall capacity constraints by reducing the scope to high-risk areas and planning a follow-up audit for the remaining areas in the next quarter. The CAE communicates the revised scope and resource plan to the board and senior management. The engagement proceeds with the adjusted scope.

© Becker Professional Education Corporation. All rights reserved.

Illustration 2 Impact of Technology Resource Limitation

During an engagement, the engagement supervisor finds the internal audit team lacks advanced analytics tools to efficiently analyze the large volume of transactional data. The engagement supervisor raises the limitation with the CAE, who considers the following options:

- Acquiring a data analytics tool
- Finding alternate internal resources
- Outsourcing the analytics portion of the engagement
- Modifying the engagement scope to rely on sampling techniques

After careful deliberation of the impact on the quality of assurance, sampling is ruled out, and there is no time to learn a new tool. The CAE first contacts the organization's IT department to identify whether a suitable tool and resource exists elsewhere within the organization but has no success. Due to data volume and compliance needs, an external firm is identified to co-source the analytics portion of the engagement scope, while the CAE plans to acquire and train internal audit team members on advanced tools in the next two quarters.

1.2.2 Process Improvement

The success of an engagement is usually determined based on:

- conformance with the Standards;
- achievement of engagement objectives; and
- completion within budgeted hours.

It is important for the internal audit function to make continuous efforts at improving the engagement resource planning to maximize the effectiveness and efficiency of resource implementation.

For example, internal auditors may keep track of the actual time spent performing the engagement against the budgeted time as well as solicit feedback from management and key personnel who are involved in the engagement. This may be beneficial, as the times can be reviewed to improve future resource planning.

Pass Key

Time constraints may reduce the scope of an engagement; however, time constraints should not reduce the quality of engagement work, especially in high-risk areas.

© Becker Professional Education Corporation. All rights reserved.